Compliance between Adaption and Advance

CEJ
COMPLIANCE ELLIANCE JOURNAL

ISSN 2365-3353
Volume 9 • Numbe
Spring 2023

Compliance Elliance Journal (CEJ)
Volume 9, Number 1, 2023
ISSN: 2365-3353
This version appears in print and online. CEJ is published twice per year, in spring and fall.

Title: Compliance between Adaption and Advance

Website: www.cej-online.com

E-Mail: info@hendrikschneider.eu

Address:
Taunusstrasse 7
65183 Wiesbaden, Germany

Telephone: +49 611 95008110

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

Compliance between Adaption and Advance

TABLE OF CONTENTS

EDITORIAL

COMPLIANCE BETWEEN ADAPTION AND ADVANCE

Compliance organization and compliance function must constantly evolve and be adaptable, both through further development within the company and changes in the political and legal situations in which companies operate. In this issue, we kick off with a piece of thought in which Michele DeStefano (Content Curator) engages with experts from compliance practice, including Markus Endres (Advisory Board CEJ) on the question: What role can and should compliance play in digital transformation in the enterprise? From a legal perspective, it is clear that determining the "role" of compliance is exceedingly relevant, if only because of liability.

Furthermore, our authors in this issue deal with the "Monaco Memo" and its significance for antitrust investigation in the USA and with the continuing relevant topic of sanctions compliance. In addition, our authors from Austria and Liechtenstein describe the implementation of an effective compliance management system in the company and the Compliance Officer's duty to monitor.

We aim to continue the debates on the development of compliance and are interested in papers from all over the world. We eagerly await your respective impulses and hope you enjoy reading!

With our best regards,

Michele DeStefano, Konstantina Papathanasiou & Hendrik Schneider
Content Curators of CEJ

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

THE UNCONSCIOUS CONSCIENCE OF DIGITAL TRANSFORMATION: THE CHIEF COMPLIANCE OFFICER?

A Thought Piece

Michele DeStefano, Isabel Parker & Giorgia Vulcano

AUTHORS

Michele DeStefano is a Professor of Law and the Larry Hoffman Greenberg Traurig Business of Law Chair at the University of Miami School of Law, a Program Chair and an Affiliated Faculty member at the Harvard Law School Executive Education Program, and an Affiliated Faculty member at IE Law School. She is also the Founder of LawWithoutWalls, Founder and Content Curator of the Compliance Elliance Journal, and a Co-creator and Chief Faculty Advisor of the Digital Legal Exchange.

Isabel Parker is a Partner in Legal Management Consulting at Deloitte Legal and also a Faculty Advisor at the Digital Legal Exchange, a non-executive Board Member at the College of Legal Practice. She has extensive experience in the legal market and was formerly an associate and later the Chief Innovation Officer at Freshfields Bruckhaus Deringer.

Giorgia Vulcano is a US/European lawyer with a background in human rights and international law. She has worked in both global organisations and digital start-ups across Latin American and Europe, helping cross-functional and cross-cultural teams define the legal path to develop and innovate in a sustainable and human centered way. Currently, she serves as legal subject matter expert and counselor on digital ethics, innovation and data protection laws. She is a Faculty member of the Digital Legal Exchange, Board Member of W@Privacy and Education Advisory Board Member of the International Association of Privacy Professionals (IAPP).

The authors would like to thank our interviewees and participants of the Digital Legal Exchange Salon Event in February 2023 for their thoughts and contributions.

TABLE OF CONTENTS

I. INTRODUCTION

Corporations around the globe are embracing Digital Transformation ("DT") to enhance competitiveness i.e., streamline operations, strengthen relationships with customers, and increase revenue.[1]

In this dynamic digital world, where data and algorithms are increasingly leveraged both for decision-making and to achieve economic and social objectives, a relevant digital transformation requires corporations to, not only onboard new technologies and ways of working, but also to address how they will be using tech in a responsible, ethical, customer/consumer-centric, and sustainable way.[2] Necessarily, functions that directly impact the bottom line (like Sales, R&D, Supply Chain) are deeply engaged in these DT efforts.[3] The question is what role is and should Compliance be playing in these DT efforts.

This thought piece focuses on the evolving role of the Compliance function in this rapidly developing ecosystem, analyzing what role does – and should – the Compliance function play in DT and how should the Compliance function future-proof itself to better manage the governance, risk, and compliance (GRC) aspects of their corporation's DT initiatives and better leverage the environment, social, and governance ("ESG") objectives of their company.

To address these questions, the authors interviewed two heads of Compliance at larger multinational corporations and facilitated a Salon hosted by the Digital Legal Exchange, entitled "The Role of Compliance In Digital Transformation: Old Habits Risk Harm". This event was attended by 12 participants including several General Counsel and Compliance professionals. The Salon was conducted under the Chatham House rule. All participants consented to an anonymised write up for these purposes.[4]

The purpose of this piece is to provoke more international, cross border discussion around the role of Compliance in digital transformation.

[1] For a description of Digital Transformation and the role of General counsel and inhouse legal departments (which often have oversight over Compliance departments), see generally Michele DeStefano, Bjarne P. Tellman & Daniel Wu, *Don't Let the Digital Tail Wag the Transformation Dog: A Digital Transformation Roadmap for Corporate Counsel*, 17 J. Bus. & Tech. L. 183 (2022).

[2] Id. at 197-201; id. at 202 (explaining that "[i]n today's corporate environment, legal functions are expected to digitally transform in harmony with the multi-national corporation itself in order to deliver services that are . . . increasingly proactive, client and customer centric, data and metrics driven, tech-enabled, collaborative, and agile, purpose-focused, and where possible, revenue generating").

[3] Shrubs Balsubramanian, *Digital Transformation for the Risk and Compliance Functions*, Deloitte (2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-digital-transformation-for-the-risk-and-compliance-functions.pdf (last visited April 10, 2023).

[4] A general, anonymized, description of all participants/interviewees' titles and companies is on file with the authors and available upon request.

II. COMPLIANCE´S ROLE IN DIGITAL TRANSFORMATION EFFORTS

A. Baking in Compliance at the start

Unlike Sales, R&D, Supply Chain, Marketing, and other functions, Compliance and Legal are not always included in, or considered critical to, enterprise DT efforts. Instead, work is done in silos and compliance approval is sought late in the game, sometimes too late.[5] Consider the following example:

Let's say the Human Resources ("HR") function wants to launch a new tool to assess employees against a number of different factors to help determine whether their performance merits a promotion or change of role. Traditionally, this is something that HR would design and decide as a function before involving other partners. The HR team may be well-intentioned and their goal is simply to create a fairer and more equitable way to assess employees. However, during the development and planning phase, the HR function may not be considering the legality of using such a tool in all the countries in which the company operates (such as Germany, for example, which is generally very strict) despite the fact that the EU's General Data Protection Regulation ("GDPR")[6] and California's Consumer Privacy Act ("CCPA")[7] regulate how a company collects and handles not only consumers' but also employees' data.[8] In other words, at this point the G in ESG (Environment, Social, and Governance) is not top of mind.

Even if the tool complies with regulations and processes data only for the employment purposes that employees have consented to, the HR team may not be thinking about whether it is "right" or "ethical" to use this kind of tool: Does it accord with the company's stated values relating to the data privacy of employees? Does it align with the company's commitments to the S in ESG, by upholding the social responsibility to protect and respect the privacy of employees', consumers,' partner's, and investors' data whenever that data is collected and processed? Whether the project crosses a threshold legal data protection line or an ethical one, compliance generally isn't involved until after the development phase, at which point they will be asked to assess the project, identify the risks, and suggest remediations. This is true even when the company has a privacy or data ethics officer. By contrast, the IT team is often involved at an early stage, as the team is considered an essential part of the decision-making process whenever a technology solution is purchased or developed. But professionals within companies often do not consider Compliance involvement to be critical to the process, or at least not

[5] Balsubramanian, *supra* note 3, at 2.
[6] *See generally*, General Data Protection Regulation (GDPR), https://gdpr-info.eu/ (last visited April 8, 2023).
[7] *See generally*, California Consumer Privacy Act (CCPA), https://www.oag.ca.gov/privacy/ccpa (updated February 15, 2023) (last visited April 8, 2023).
[8] *See e.g.,* Sara H. Jodka, *The GDPR Covers Employee/HR Data and It's Tricky, Tricky (Tricky) Tricky: What HR Needs to Know, Dickeson Wright*, HRDickensonWright (April 3, 2018), https://hr.dickinson-wright.com/2018/04/03/gdpr-covers-employeehr-data-tricky-tricky-tricky-tricky-hr-needs-know/?utm_source=mondaq&utm_medium=syndication&utm_term=Employment-and-HR&utm_content=articleoriginal&utm_campaign=article; Tully Rinckey, *Responsibilities of Employers under the General Data Protection Regulation*, Lexology =https://www.lexology.com/library/detail.aspx?g=f19963f0-3be2-485c-88d5-dceaece4b446 (last visited April 8, 2023); Peter Todorovski, *Employee Data Processing: What is Right and Wrong Under the GDPR*, PrivacyAffairs (April 7, 2023), https://www.privacyaffairs.com/employee-data-processing/#:~:text=GDPR%20is%20not%20as%20specific%20about%20processing%20employees%E2%80%99,the%20processing%20of%20employees%E2%80%99%20data%2C%20including%20sensitive%20data; *California Consumer Privacy Act: Employee and B2B Exemptions Expire January 1, 2023*, Morgan Lewis (October 14, 2022), https://www.morganlewis.com/pubs/2022/10/california-consumer-privacy-act-employee-and-b2b-exemptions-expire-january-1-2023#:~:text=The%20CCPA%20currently%20imposes%20limited%20obligations%20on%20employers,employees%2C%20job%20applicants%2C%20officers%2C%20directors%2C%20and%20independent%20contractors.

in the "concept phase" of the project. Instead, they recognize that there may be some considerations to take into account, but believe that Compliance and Legal are there to flag them later.[9] Therefore, the development process generally proceeds with HR working with IT to develop or purchase the tech, negotiate with a vendor to on board the solution or collaborate with a development team to design it. Legal or Compliance, on the other hand, are brought into the process late in the day, often raising the legal and/or ethical flags that—as a matter of due course—slow down or sometimes even block the whole project.

This reactive approach (and late involvement of Compliance and/or Legal) is not only due to the attitudes and behaviors of the HR professionals in this example above. Legal and Compliance departments themselves also bear some responsibility for the outcome: often, they do not see their role as being part of the creative and project development process. Instead, they too see themselves as there to uncover a mismatch between a legal or regulatory requirement and what the company is doing – not to propose or build a solution that has a creative element or to be part of a team to create something new. Moreover, there is often not a direct line between compliance and the IT group that develops technology (that could have potential hidden vulnerabilities).[10] Plus, the language involved in some of the technological developments is very complicated and can be challenging for a non-technical person to decode. This invariably results in lots of questions from the lawyers (which at times can be hard to formulate in a way that breaks down the complexity of the topic) that then aggravates the other professionals on the team (especially the IT professionals). On the one hand, this type of questioning by Compliance is understandable because it is extremely hard to green light a project or provide advice or assess the level of the risk without understanding how the tech works and its implications. However, on the other hand, it uncovers the need for Compliance to enhance their technology know-how given how essential it is to do their job effectively and future-proof their value creation for the business teams. To execute their role effectively, Compliance professionals need to be able to map out the technology architecture and associated data flows in order to identify a gap or risk or unintended unethical or biased consequence. They need to do so (to be adept at problem finding) so that they cannot just simply say "no" or overburden the remediation, but actually suggest a creative solution to the problem. In other words, Compliance cannot recommend that the team should implement xyz measures to prevent a certain negative consequence from happening if they don't understand how the tech works, what is the business purpose, and what are the current processes and their impact. To be sustainable and effective, the decision around what measures should be implemented as possible tweaks or fixes should reconcile compliance requirements and the consensus of the teams involved.

[9] Balsubramanian, *supra* note 3, at 2.
[10] Balsubramanian, *supra* note 3, at 2.

B. The rising importance of technological literacy and cross-functional partnership

Compliance professionals who are not technologically literate may become reliant on the IT professionals' interpretation and description of the data flows and technology architecture. The lexicon and focus of an IT professional is of course different from that of a Legal or Compliance professional. This lack of common vocabulary can create misunderstandings between professionals, which can slow down product development and result in negative consequences for the end customer. Consider a simple example like the word "bias". To an IT professional, data is biased by design and certain degrees and nuances are acceptable (if not expected) while others are not and can compromise the data. Either way the word "bias" doesn't have the same negative connotation as it does for a Legal or Compliance professional. Instead, for IT, the word "bias" is rather related to the quality of the data. However, the Compliance professional might provide advice that it is *imperative* that the data has *no* bias. This is completely unrealistic and threatens the Compliance professional's credibility with the IT professionals. So, there is a lack of common language that prevents proper advice and understanding of the scope of the risks. As a result, a stereotypical way of seeing things and proceeding is perpetuated and Legal and Compliance are brought in late in the process, positioned to throw red flags and perceived as blockers instead of professionals that can help problem-find and problem-solve.[11] This leaves Compliance viewed as cops and cost centers instead of strategic business partners[12] whilst uncovering the necessity for this function to overcome traditional, obsolete, frameworks and ways of working that no longer respond to the speed, complexity and uncertainty generated by DT. As one Chief Compliance Officer explained:

> "The function of compliance should be as a business partner which helps us to gain a very high level of trust. People have to understand that we are not the internal police force but business partner consultants who are willing and able to put ourselves in their shoes and try to make their vision into reality. And that's my understanding, that we're a business partner, not a control audit function."[13]

C. New ways of working to address regulatory fragmention

The challenges presented by this way of working are exacerbated by the significant increase in regulation and enforcement in the digital space, the broadening scope of regulation across countries around the world, and the speed at which DT is happening in most organisations.[14] Leading companies

[11] *See* Michele DeStefano, *Chicken or Egg: Diversity and Innovation in the Corporate Legal Marketplace*, 91 Fordham Law Review 1209 (2023) (explaining that lawyers lack the skillsets and mindsets of collaborative innovators and do not spend enough time problem-finding and often have a fixed as opposed to growth mindset which is not conducive to the type of collaboration and innovation corporations need from their legal professionals 1236-1239); Michele DeStefano, *Legal Upheaval: A Guide To Creativity, Collaboration, and Innovation in Law* 44-55 (John Palmer et al. eds., 2018) (explaining why lawyers lack the skillsets and mindsets of innovators and fail to proactively collaborate with empathy, inclusivity ,and an open mind). For more information on the importance of problem finding to innovation see Daniel H. Pink, *To Sell Is Human: The Surprising Truth About Moving Others* 5 (2012); Tina Seelig, *What I Wish I Knew When I Was 20: A Crash Course on Making Your Place in the World 20* (2009) (referring to problem-finding as "need finding"); Tina Seelig, in *Genius: A Crash Course on Creativity* 19–30, 95–102 (2012).

[12] *See* Michele DeStefano, *Creating a Culture of Compliance: Why Departmentalization May Not Be the Answer*, 10 Hastings Bus. L.J. 71 (2014).

[13] Interviewee/Salon Participant #2, Chief Compliance Officer of a Germany-based international pharmaceutical company.

[14] Sanjay Srivastava, *The Blistering Pace of Digital Transformation is Only Going to Get Faster*, Fortune (April 21, 2021, 3:00 P.M), https://fortune.com/2021/04/21/digital-transformation-automation-data-economy-reskilling-retraining/; John de Yonge, *The CEO*

are developing new digital products and services at a dizzying pace.[15] NFTs are a great example. In the past, a company might have years or at least a year to launch something new like an NFT, but now it's in months, in 6 weeks sprints.[16] Another example worth mentioning relates to ChatGPT: the infamous AI tool was adopted by one million users within five days of its release.[17] In contrast, when Marty Cooper, an engineer at Motorola, made the first mobile phone call in 1973, it would take 10 more years before cell phones would be made available to the average consumer.[18] The level of adoption and mainstream access to innovation has never been this fast, triggering new risks and demanding for immediate responses and more preventive approaches.

Given that DT-relevant regulatory frameworks develop quite rapidly to a remarkable maturity level, and the window for implementing regulations is decreasing, complying with increasing local requirements on a local level is one tricky task in itself. Designing and implementing group-wide and global tools that reflect all of the—often contradictory—requirements of the relevant jurisdictions can be highly challenging.

As one Chief Compliance Officer explained,

> "Being compliant when it comes to DT is very hard and that is true for different reasons and the legal complexity of all the legal fields that are linked to DT including data protection. It's pretty hard if not impossible to reach hard compliance because it is happening so quickly, and it is all so new and foreign. So for a multinational corporation, there is an additional level of complexity for being compliant. And it is even more difficult than a cross border check. . . . Multinational companies have to concern themselves not just with GDPR but laws in all the different countries the company has offices in and does business."[19]

A further complication is fragmentation. Different jurisdictions are taking radically different approaches to enforcement. One example is the recent action against Meta, under which Meta was fined €390 Million by the Irish Data Protection Commission ("DPC") after it adopted the finding by the European

Imperative: How Has Adversity Become a Springboard to Growth?, EY (March 8, 2021), https://www.ey.com/en_us/ceo/the-ceo-imperative-how-has-adversity-become-a-springboard-to-growth (reporting that 61% of CEOs "plan to undertake a major new transformation initiative").

[15] Microsoft CEO Satya Nadella claimed that the first two months of the COVID-19 lockdowns forced corporations such as Microsoft to digitally transform more in two months than they had in two years. Jared Spataro, *2 Years of Digital transformation in 2 Months,* MICROSOFT (April 30, 2020), https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/.

[16] Simon Blackburn et al., *Digital Strategy In A Time Of Crisis,* McKinsey Digital (April 22, 2020), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-strategy-in-a-time-of-crisis. Note, research suggests that the pace of technology adoption is faster in the United States than in some other countries. In terms of AI readiness, for instance, a 2019 McKinsey survey found that the U.S. led the world in AI readiness, due to its strong AI ecosystem and positive ICT connectedness. *See also* Jacques Bughin et al., McKinsey Glob. Inst. Notes from the AI Frontier: Tackling Europe's Gap in Digital and AI 2 (2019) (finding that Europe lags behind the U.S. and China in digitization and adoption of AI).

[17] Katharina Buchholz, *ChatGPT Sprints to One Million Users*, Statistica (January 24, 2023), https://www.statista.com/chart/29174/time-to-one-million-users/.

[18] Kevin Lync, *1973: First Mobile Phone Call*, Guinness World Records (August 19, 2015), https://www.guinnessworldrecords.com/news/60at60/2015/8/1973-first-mobile-phone-call-392969.

[19] Interviewee/Salon Participant #2, Chief Compliance Officer of a Germany-based international pharmaceutical company.

Data Protection Board ("EDPB") that Meta's "performance of contract" basis for collecting and processing data for personalized advertising was non-compliant with GDPR.[20] Organizations are being compelled by decisions like these to take accountability for protecting consumers and also for providing more transparency. At the same time, consumers are increasingly aware of their own rights with respect to their data, and less willing to entrust it to third parties.[21] As many participants in the Digital Legal Exchange Salon Event ("DLEX") explained, COVID-19, and the requirements to share data on, for example, vaccination status, heralded a shift in the level of trust that individuals are prepared to place in organizations who are handling their data. As one Chief Compliance Officer explained,

> "It is a jigsaw puzzle of different legal requirements and regulations and my current understanding is that it is impossible to identify and set up and run group-wide processes and tools that actually comply with data protection rules in every level in every country. So we are only talking about harsh compliance and we can pretty much not think about ethics yet."[22]

Plus, there is a gap between what the community thinks is a 'normal' digital life and what the data protection authorities consider lawful. This gap creates a complex tension. Consider that a few weeks ago, the highest data protection authority in Germany ordered the German government to take down its facebook site, and the government refused despite the order. As a result, the Compliance Officer felt compelled to begin internal discussions with his colleagues. He explained to them that

> "this is an absurd situation, that there is a legal requirement on the German government that the government itself is refusing to follow! This begs the question: do we want to and can we use Facebook in our company?"

These are the types of conversations Compliance is having inside their companies because, unfortunately, these kinds of gaps between consumer desires and the legal requirements are a burden to DT in large corporations. It makes it almost inevitable that compliance professionals involved in data protection are seen as slowing things down—because they do, often through no fault of their own. They have to. As this Compliance Officer explained,

> "when it comes to anti-corruption policies, I can apply compliance as a business partner and they accept our recommendations and people like and value what we do for the organization. But when it comes to data protection, where there are a set of rules and regulations that people can't relate to, we have a massive loss of trust as a compliance community. We are considered

[20] Meta Fined €390 Million by Irish DPC for Alleged Breaches of GDPR, Including in Behavioral Advertising Context, The National Law Review (January 20, 2023), https://www.natlawreview.com/article/meta-fined-390-million-irish-dpc-alleged-breaches-gdpr-including-behavioral#:~:text=As%20a%20result%20of%20the%20investigations%2C%20the%20DPC,publishers%20engaged%20in%20behavioral%20advertising%20in%20the%20EU (explaining that the DPC original did not find that Meta was legally noncompliant for relying on the "performance of contract" bases but instead that and that "it did not clearly disclose its purpose for collecting and its usage of the data."); Jennifer Bryant, *Irish DPC Fines Meta 390M Euros Over Legal Basis for Personalized Ads*, IAPP (January 4, 2023), https://iapp.org/news/a/irish-dpc-fines-meta-390m-euros-over-legal-basis-for-personalized-ads/.

[21] According to 2023 the *International Association of Privacy Professional Privacy and Consumer Trust Report*, "[n]early 68% of consumers throughout the world said that they are either somewhat or very concerned about their online privacy. This concern affects how much they trust companies, organizations and governments to collect, hold and use their personal data. Consumers make choices based on their perceptions of privacy, adjusting their compasses in a world awash in data by deleting apps, withholding information and avoiding purchases when they feel their privacy is at risk." Müge Fazlioglu, *International Association of Privacy Professional Privacy and Consumer Trust Report* (March, 2023), https://iapp.org/resources/article/privacy-and-consumer-trust-summary/.

[22] Interviewee/Salon Participant #2, Chief Compliance Officer of a Germany-based international pharmaceutical company.

> the poor guys that are suffering under an unrealistic, unpractical data protection regulation that we are enforcing over them. However, I don't see an alternative approach. As long as we are facing a legal requirement that is way off the people's reality, like the Facebook situation, it is a gap that hardly can be filled. I can't waive my legal reasons even if I understand that it helps the business and is a good DT vision. I can't say let's go for it if it is not compliant."[23]

So, this leads to even more siloed working. If Compliance handles things in a non-practical and non-sustainable way (to the letter of the law that doesn't fit with the company's values, or align with what people at the company or its customers value), data privacy will be perceived as a burden and as a topic with little practical relevance. This could have the unfortunate consequence of relegating Compliance professionals to an enforcement role, rather than viewing them as equal contributors.

Many of the DLEX Salon participants expressed that siloed ways of working are also a threat when it comes to cybersecurity. The cyber threat landscape presents another transformation challenge for Compliance professionals. As the volume of data and the use of technology increases, so does the threat of cyber-attacks and the attention of regulators.[24] The business expects Compliance teams to respond by becoming increasingly mature in assessing and preventing cyber risk. This requires, again, a high level of alignment across business teams, and a high degree of multidisciplinary working. Compliance needs to be right at the heart of these efforts.

True, more and more, executives are recognizing the problem with the siloed, isolated approach and that a more integrated collaboration is needed between the IT, Product Development, Merchandising, Marketing, Legal and Compliance departments. However, as another Compliance Officer explained,

> "very few have figured out how to unblock it and it is unclear how to achieve that given that there is not yet an understanding of what is blockchain, let alone trying to find a more integrated way of working."[25]

This leads to, not only legal risks, but also an ethical slippery slope which can negatively impact the customer. It often falls to the Compliance professionals to consider not just the legal compliance aspects of DT but also how to further the corporation's values and to protect the customer's wants and needs with respect to use of consumer data. This is the focus of the next section of this paper.

[23] Interviewee/Salon Participant #2, Chief Compliance Officer of a Germany-based international pharmaceutical company.
[24] See generally, The Cyber-Threat Landscape: The Digital Rush Left Many Exposed, PWC US Digitatl Trust Insights Snapshot Survey (2021), https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/2021-digital-trust-insights/cyber-threat-landscape.html (last visited April 10, 2023).
[25] Interviewee #1, Global Data Ethics Manager of a multinational beverage and brewing company.

III. UNCONSCIOUS PROBLEM WITH COMPLIANCE´S CURRENT ROLE

A. Operationalizing purposeful innovation and digital ethics

The mission and responsibilities of Compliance are evolving beyond just compliance. Yes, its job is to make sure the company's DT efforts and use of data are aligned with the rules and requirements applicable to the corporation. However, Compliance professionals are not solely responsible for the corporation respecting the law but also for enforcing the company's values (such as DE&I) and ensuring the technology the company is developing can be used to optimize the company's risk management. Furthermore, they are responsible for detecting and addressing the ethical aspects including the real and potential unintended consequences of the projects that a company may launch and also what customers would expect from a trusted organization handling their data.

In our digital world, where product and service choice and convenience offer in the marketplace is at its peak, customers have the option and awareness to give their money and their information to companies that they trust. They are empowered to expect that these companies are living up to their promises to implement a meaningful, purpose-driven, transparent privacy program that includes collection limitations that demonstrate its commitment to its customers' privacy. The opposite, however, is also true. Those companies that don't go further than what is legally required will lose their customers where a competitor is offering more. According to a recent McKinsey report analyzing digital trust, consumers "consider trustworthiness and data protections to be nearly as important as price and delivery time."[26]

Innovation and transformation require flexibility and a "trial and error" approach, which Compliance functions are traditionally adverse to. However, faced with increasingly uncertain and complex scenarios (from both a technological and regulatory perspective), exploring concepts such as user empathy (which is native in Design Thinking methodology) and Agile, can become new tools to address the needs and aspirations of clients and customers.

Importantly, in some ways it appears that the person that is driving the ethical conscience of the company is the Chief Compliance Officer who is doing so almost unconsciously (without the company being conscious of it). And the Chief Compliance Officer is a good fit for this role, in part, because there is so much left unaddressed in the complex overlapping regulations. For example, questions remain around how to group and tag data, about the social and ethical use of group data versus that of an individual, and also how a person is tracked and targeted based on their online activity.[27] Consider for example a cookie banner. There are certain requirements a company has to meet from a data protection standpoint, but nothing prevents a corporation from using certain types of patterns that are known to help nudge customers into accepting vs rejecting a clickable advertisement. Similarly, nothing requires the company to use certain fonts or colors to make something more visually accessible to people with impairments. Today, forward thinking Compliance Officers consider these types of concerns part of their job and critically important to their company's DT efforts.

[26] Jim Boehm, Liz Grennan, Alex Singla, and Kate Smaje, *Why Digital Trust Matters*, McKinsey & Co. (September 12, 2022), https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters.

[27] Taylor, L., Floridi, L., & Van der SLoot, B (Eds.) *Group Privacy: New Challenges of Data Technologies* (Vol. 126) (2016); Lillian Edwards, *Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling*, L Edwards Law, Policy, and the Internet (Hart 2018) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3183819.

Given their role in cybersecurity and data protection, Compliance professionals are, of course, involved in updating data protection policies and privacy notices. However, privacy notices are often updated without talking to the customers i.e., to consider what matters to them, and how and when they want these notices, if at all. Currently, reliance is put on opinions, i.e., what consumers SAY they will do if a company is subject to a data breach. Forward thinking Compliance Officers, however, see the act of updating data protection policies and privacy notices, as an opportunity to help their company be more client-centric. Instead of relying on opinions (which can end up validating things that are assumed), they seek user validation by analyzing the data to determine, for example, whether more transparency or more data protection measures really impact behavior. They seek more than simply validating a privacy notice or ensuring that the notice is changed to meet the right glocal rules and regulations, they seek to find out what matters to consumers so that the updates and the overall user experience provide consumer value.

Consider third party advertising. It is a disputed field when it comes to what is allowed legally and ethically. If a person visits website #1, this data can be selected and sold to a completely different third party and the same third party then can use it for their own ads. Forward thinking Compliance Officers at progressive companies who are dedicated to ensuring their customers trust the way they use their data (and believe it will make a difference in purchasing behavior by customers) are trying to go one step further than simply ensuring legal compliance. They are thinking deeply and strategically about the issues related to third party advertising and whether the selling of that data to third parties is ethical and in line with the values of the company. They are also considering whether such advertising has the right type of messaging and transparency around it, so as to not breach the company's commitment and consumer's expectations.[28] Similarly, forward thinking Compliance Officers are having discussions with Marketers within the company who can track users' activity to provide a personalized, customized experience which, on the one hand, might delight the customer. As such, privacy and data protection can be a force for good, in improving the user experience, particularly when the focus is on using only the data that is needed and processing it in a way that consumers can reasonably expect and appreciate. However, on the other hand, even if the company has taken the right steps before collecting the information,[29] using it in this way, it might make them worried about their privacy and scare them away. In the era of surveillance capitalism,[30] if a company suddenly puts an ad up in front of a customer of one of its products that might relate to their activity, it might put people off. In fact, sometimes it even raises concerns for people because they do not understand how the data stream is working. They may even think their computers or phones are being watched, listened to or tapped by the company that has now put the advertisement in front of them which can create people to distrust a company and walk away. However, as one Compliance Officer explained,

> "the common denominator across regulation in the digital space is transparency. Not only do organizations need to be compliant, they also need to be able to explain their approach and

[28] To Personalize or Hyper-Personalize? The Paradox of Privacy and Targeted Advertising, Ardent Privacy Blog, https://www.ardentprivacy.ai/blog/to-personalize-or-hyper-personalize-the-paradox-of-privacy-and-targeted-advertising/ (last visited April 8, 2023).

[29] Id. ("Online marketers also need to be aware of how data privacy laws regulate their practice. Laws such as the EU's GDPR, California's Consumer Protection Act (CCPA), California Privacy Rights Act (CPRA), and Virginia's Consumer Data Protection Act (CDPA) currently regulate the collection and sharing of data, which requires companies and marketers to take certain steps before collecting information and using it for marketing purposes.").

[30] John Laidler, *High Tech is Waiting for You: Q&A with Shoshana Zuboff*, Harvard Gazette (March 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/.

actively to demonstrate compliance. In this way, regulation demands an ethical response, not simply a response that is compliant."[31]

B. The rising implications of ESG

Similarly, ESG frameworks are changing, to take into account the tensions between cybersecurity, digital ethics and privacy—which are new and emerging elements in the ESG reporting space.[32] This reporting obligation presents its own challenge: how can the value of data ethics and the safeguarding of privacy be measured? What metrics can be used to validate success? How can companies measure and communicate cultural change and new ways of working? Data Ethics and Compliance professionals will be challenged to define the metrics that can evidence the value they bring to the business. But as all the participants in the DLEX Salon event agreed: Evidencing a return on the internal investment required for digital ethics is challenging. However, as the unconscious conscience of the company, it is the Compliance Officer's job, in collaboration with other functions, to start to develop the metrics to measure and determine if there is a business case for ethical compliance that is in line with the corporation's values and promises (and that goes above and beyond the letter of the law).

IV. CONCLUSIONS AND A FEW RECOMMENDATIONS

That Compliance Officers are taking on this role is laudable and sensible. As others have remarked, they have the motivation and ability to be the conscious of the company, to ensure that considerations beyond the letter of the law (ethics, and consumer desires and preferences) are taken into account from the beginning during the problem—and opportunity—finding stages and all the way through all phases of product development and launch. Yet, the current siloed ways of working have consequences that make it almost impossible for the Compliance Officer to do a good job of being that unconscious conscience. This is due to a few factors.

First, like the other department heads, Compliance Officers also often have limited access to data, they are focused on their individual department mandates, and they cannot always look at risk signal data holistically and go beyond what is legal to what is ethical.[33] As such, as others have pointed out, sometimes Compliance only has access to "a limited data set that is directly related to compliance. . . [T]hese data silos often keep risk teams from seeing the complete picture."[34] As the Chief Ethics & Compliance Officer at a multinational technology company shared, "One challenge is access to data and gaining support from the IT function."[35] The participant's organization "has grown through acquisition, and data integration has been complex. They are working to apply AI to enable proactive fraud analytics across the business; however, progress is hampered by access to the IT function, as compliance as a function is not IT's highest priority."[36] Although agreeing, the Global General Counsel for

[31] Interviewee #1, Global Data Ethics Manager of a multinational beverage and brewing company.
[32] See BlackStone, ESG Policy, https://www.blackstone.com/wp-content/uploads/sites/2/2022/02/BX-Firmwide-ESG-Policy.pdf) (last visited April 7, 2023).
[33] Sean Thompson, *Why the Next Era in Risk Management and Compliance Requires Digital Transformation*, Forbes (November 9, 2022), https://www.forbes.com/sites/forbesbusinesscouncil/2022/11/09/why-the-next-era-in-risk-management-and-compliance-requires-digital-transformation/?sh=7c4af0c7e351.
[34] *Id.*
[35] Salon Participant #12, VP, Chief Ethics & Compliance Officer at a Fortune 500, multinational technology company.
[36] *Id.*

a global engineering company explained the catch 22 that some are facing "a tension between the requirement on organizations to demonstrate transparency and accountability and an increased trend towards data localization. It is challenging to digitally transform if data is 'locked down' and not accessible to mine for insight."[37] In other words, the right governance ensures that processes and policies are in place to help digital efforts scale and make them accessible across different teams and jurisdictions, but data is a critical enabler. It is the key to helping uncover common pain points, to validate trends, and to ensure consistency across different business lines and jurisdictions.

Second, the siloed way of working prevents cross-functional teams that understand each other's ways of working and also prevents a consistent approach across jurisdictions which is critical. Organizations need a unified standard to allow them to measure and compare levels of risk. This requires a high degree of alignment across the business, and a high level of consensus. Only with that, will teams have accountability i.e., clarity as to who has accountability for processes and outcomes.

Third, with the existing silos and negative consequences mentioned above, it is near impossible to demonstrate value. Evidencing a return on the internal investment required for digital ethics is challenging. It is akin to a cultural transformation, having a long lead time before it will bear fruit. Building a business case based on this intangible value is impossible with the current siloed approach. Similarly, measuring objectives and achievements for digital ethics and ESG in the context of compliance is a challenge.

As one of the participants of the DLEX Salon aptly explained,

> "in order for the Compliance Officer to move beyond being seen in traditional 'policing' role and be able to use the data and technology to transform the business, and develop a coherent business case in support of the change, the Compliance Officer needs the authority to create proofs of concept; and, more than that, it needs senior sponsorship, and a high level of collaboration with the support by other teams in the business to work together to effect large scale, transformational change."[38]

Only then, will Chief Compliance Officers be able to spearhead projects that provide the company insights that allows them to map risks based on the type of asset and the nature of the risk and identify gaps that need to be addressed, leverage data to find patterns and areas that require intervention to prevent anti-corruption, and most importantly, help operationalize ethical and customer-centric principles across the business, making the abstract principles concrete so that everyone is working to not only comply with the law but also to meet and exceed expectations of clients.

Lastly, the ultimate goal is that the role of the Compliance Officer, that may be currently an unconscious conscience of the company, be out in the open and, more than that, embedded in all functions of the company. It is imperative that the departments across companies do not solely rely on Compliance to catch or fix the ethical issues but to design projects that embed the ethical conscience when handling the data to create that value for consumers. As a Senior Corporate Legal Counsel of a global bank who participated in the DLEX Salon, explained,

[37] Salon Participant #9, Global General Counsel of a Fortune 500, multinational corporation engineering, electrification, and automation company.
[38] Id.

> "Digital transformation is the responsibility of the entire enterprise. Marrying compliance with digital transformation is particularly challenging. It cannot be reduced to individual KPIs. instead, each individual has to take accountability for a compliant transformation, with all employees being taught how to manage risk in an ethical way."[39]

As noted earlier, this essay is merely a thought-piece, based on a limited amount of research and a lot of qualitative and anecdotal evidence. That said, our purpose is aspirational and so we conclude on an aspirational note with a quote by one of the Chief Compliance Officers we talked to:

> "Being compliant is the base element of being ethical but there is so much more. That's why being a Compliance professional right now might be the best job in the world especially if you are a Lawyer Compliance professional because then you are not the person only reviewing the provisions of a contract. Instead, you get to help people fulfill a future position in a safe and ethical way and that is very motivating and drives me."[40]

[39] Salon Participant #5, Senior Corporate Legal Counsel of a multinational financial services company.
[40] Interviewee/Salon Participant #2, Chief Compliance Officer of a Germany-based international pharmaceutical company.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

THE MONACO MEMO AND IMPLICATIONS FOR NAVIGATING ETHICAL ISSUES IN ANTITRUST INVESTIGATION

Lauren E. Briggerman & Surur Fatema Yonce

AUTHOR

Lauren Briggerman is Vice Chair of law firm Miller & Chevaliers Litigation department and Lead of the Cartel Investigation & Litigation practice. She focuses her practice on white collar defense in criminal and civil matters and writes and speaks frequently on cartel and other white collar issues. She represents corporations and executives in government investigations and criminal litigation, including in the areas of criminal antitrust, bribery and corruption (FCPA), money laundering, financial services/bank fraud, and government contracts fraud, among others. She is also a founding member of the Women's Antitrust Forum, a Washington, DC-based organization that brings together women antitrust practitioners for professional development purposes. In addition, she is an active member of the Women's White Collar Defense Association and American Bar Association's Cartel and Criminal Practice Committee and serves as Vice Chair of the Compliance & Ethics Committee in the ABA's Antitrust Law Section.

Surur Fatema Yonce is Senior Associate in the Litigation department of Miller & Chevalier where she represents corporate and individual clients from a broad range of industries in government enforcement, litigation, and white collar matters. She has experience representing clients before the U.S. Department of Justice (DOJ), Securities and Exchange Commission (SEC), and Congress in investigations involving the Foreign Corrupt Practices Act (FCPA), securities fraud, and wire fraud, and in related investigations before international regulatory bodies in both the United Kingdom and Europe. She has also managed internal investigations into whistleblower allegations.

TABLE OF CONTENTS

I. OVERVIEW OF THE MONACO MEMORANDUM

In October 2021 and September 2022, Deputy Attorney General (DAG) Lisa Monaco issued remarks and a memorandum (collectively referred to as the "Monaco Memorandum" or the "Memorandum") revising the U.S. Department of Justice's (DOJ) existing Corporate Enforcement Policy.[1] DOJ's Corporate Enforcement Policy sets forth a package of carrots and sticks to incentivize companies to voluntarily self-report corporate misconduct to the government.[2]

The Monaco Memo applies DOJ-wide. It directs the components of DOJ that do not have formal policies incentivizing self-disclosures to implement such policies consistent with the standards outlined in the Memorandum. DOJ's Antitrust Division (the "Division") has a unique and long-standing Leniency Policy[3] which grants full immunity from criminal prosecution to companies that report criminal antitrust misconduct to the Division and fulfill certain other requirements. As the Antitrust Division's Leniency Policy was last updated shortly before DAG Monaco's directive in June 2022, it remains to be seen whether the Division will issue a revised policy with greater clarity and enhanced incentives to voluntarily self-report, cooperate, and remediate as the Criminal Division did in early 2023.

The Monaco Memorandum includes certain key policy revisions that are relevant to ethical considerations in investigations, namely:

Prioritizing Individual Accountability: The Memorandum states that DOJ's "first priority" in corporate criminal enforcement is to hold individuals accountable.[4] Underscoring this priority, the Memorandum directs prosecutors to resolve individual investigations before or simultaneously with corporate investigations.

Full, Timely Disclosure about All Relevant Individuals: The Memorandum reinstates the requirement from the 2015 Yates Memorandum, which requires corporations to provide DOJ with *all* relevant facts about *all* individuals responsible for the misconduct at issue.[5] This is a renouncement of the Trump Administration's policy of permitting companies to gain cooperation credit for identifying only individuals *substantially* involved in the criminal conduct. Furthermore, timeliness is critical, as delayed dis-

[1] Memorandum from Deputy Att'y Gen. Lisa O. Monaco, to Asst. Att'y Gen. Crim. Div., et al. (October 28, 2021) ("Monaco Oct. 2021 Mem."), https://www.justice.gov/d9/pages/attachments/2021/10/28/2021.10.28_dag_memo_re_corporate_enforcement.pdf; Deputy Att'y Gen. Lisa O. Monaco Gives Keynote Address at ABA's 36th Nat'l Institute on White Collar Crime, U.S. Dep't of Justice (Oct. 28, 2021) ("Monaco Oct. 2021 Remarks"), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute; Memorandum from Deputy Att'y Gen. Lisa O. Monaco, to Asst. Att'y Gen. Crim. Div., et al. (Sept. 15, 2022) ("Monaco Sept. 2022 Mem."), https://www.justice.gov/opa/speech/file/1535301/download; Deputy Att'y Gen. Lisa O. Monaco Delivers Remarks on Corporate Crim. Enforcement (Sept. 15, 2022) ("Monaco Sept. 2022 Remarks"), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement; U.S. Dep't of Just., Just. Manual §9-28.000(2015).

[2] E.g., U.S. AQorney's Manual, 9-47.120 – Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy (Jan. 2023), hQps://www.jus@ce.gov/opa/speech/file/1562851/download<hQps://www.jus@ce.gov/opa/speec h/file/1562851/download

[3] U.S. Dept. of Just., Just. Manual §7-3.300 (June 2022).

[4] Monaco Sept. 2022 Mem. at 2

[5] Monaco Oct. 2021 Remarks (emphasis added).

closure has impeded the DOJ's cases against individuals due to factors such as the running of statutes of limitations, the availability of evidence, and "the fading of memories."[6] The Memorandum emphasizes that companies place their eligibility for cooperation credit in jeopardy when they identify, but delay disclosure, of significant facts.[7]

Corporate Recidivism: The Memorandum takes a broader view of corporate recidivism for the purposes of assessing aggravating factors. Under the new "holistic approach," prosecutors must consider all prior misconduct by a corporation, including foreign, criminal, civil, and other regulatory enforcement actions against both the company and its affiliates. The Memorandum directs prosecutors to assign varying weights to each prior instance when considering a corporation's past misconduct. The most heavily weighted cases will be recent U.S. criminal resolutions (defined as less than 10 years old) and prior misconduct involving either the same personnel or management structure.[8] Furthermore, violations within heavily-regulated industries should be considered within the context of similarly-situated companies. Despite these caveats, the Memorandum makes clear that repeat offenders will be penalized because repeated misconduct is indicative of a corporation's failure to establish an appropriate compliance culture, while also acknowledging that not all instances of misconduct are created equal.[9]

Timely Voluntary Self-Disclosure: The Memorandum directs all DOJ components to establish policies confirming that, absent the presence of aggravating factors, DOJ will not seek a guilty plea in a corporate enforcement matter where the corporation voluntarily self-disclosed the misconduct, fully cooperated with the Department's investigation, and timely and fully remediated the criminal conduct.[10] It further instructs each component to define aggravating factors, which the Antitrust Division has yet to do.

Cooperation: The Memorandum cites cooperation as a mitigating factor that will be measured by degree and the company's demonstration of its commitment to cooperate. To receive cooperation credit, companies must timely preserve and disclose relevant documents located both within the United States and overseas. Thus, the Memorandum puts the burden of establishing the existence of foreign data privacy laws impeding disclosure upon corporations. Furthermore, it threatens an adverse inference against companies that appear to be capitalizing on foreign data privacy laws to shield themselves from investigation.

Compliance Program Assessment Related to "Compensation Structures," "Personal Devices," and "Third Party Applications": Consistent with the Antitrust Division's existing compliance guidance, the Memorandum emphasizes that DOJ should assess the effectiveness of a corporation's compliance program both at the time of the offense and time of charging decision.[11] The Memorandum identifies two additional metrics for evaluating a corporate compliance program: compensation structures and the use of personal devises and third-party applications for business. On compensation structures, the Memorandum directs prosecutors to consider whether compensation systems are crafted in a way

[6] Monaco Sept. 2022 Remarks.
[7] Monaco Sept. 2022 Mem. at 3.
[8] Id.
[9] Monaco Sept. 2022 Mem. at 5.
[10] Monaco Sept. 2022 Mem. at 7.
[11] Id. at 9.

that incentivizes compliance and deters risky behavior by imposing financial consequences for misconduct.[12] This includes provisions for retroactive discipline such as the claw back of compensation, and whether a company has taken affirmative steps to claw back compensation of current or former executives involved in the misconduct.[13] On personal devices and third-party messaging applications, the Memorandum instructs prosecutors to consider whether the corporation has effective policies and procedures in place to govern the use of personal devices and third-party messaging platforms such as WhatsApp or WeChat in order to ensure that business-related communications are appropriately preserved and that a company seeking cooperation credit can actually collect such communications in response to investigative requests.[14]

In this article, we discuss critical ethical considerations for internal investigations into potential antitrust violations in light of this new guidance and provide suggestions for outside counsel in managing potential legal, ethical, and practical issues. In particular, we focus on how to navigate investigations that may implicate wrongdoing by the general counsel or members of a company's board of directors to whom outside counsel reports. In these circumstances, clearly identifying and zealously representing the interests of the client entity (whether a company or a board) while effectively managing ethical issues raised by employees and board members is key to maintaining the integrity of the investigation.

II. ETHICAL ISSUES IN ANTITRUST INVESTIGATIONS IMPLICATED BY THE MONACO MEMORANDUM

A. Whether or Not and When to Disclose?

As a corporation considers whether to self-report potential criminal antitrust misconduct, certain aspects of the Monaco Memorandum implicate ethical considerations. Importantly, the Memorandum and the Antitrust Division's Leniency Policy provide much less predictability in the event of self-disclosure than the more recently published Criminal Division Corporate Enforcement Policy. The Memorandum leaves the weighing of many factors to prosecutors' discretion when crafting resolutions, leaving little ability to make inferences as to which factors will impact the ultimate form of a resolution. For example, the Memorandum does direct each DOJ component to adopt a policy that offers the presumption of a declination in the event of voluntary self-disclosure absent aggravating circumstances, full cooperation, and full remediation. However, the Antitrust Division, unlike the Criminal Division, has not yet defined "aggravating factors."

In addition, counsel cannot in good faith advise their clients to expect successive declinations for similar conduct. DAG Monaco has made clear that DOJ disfavors repeat declinations. Corporations with a history of recidivism may remain wary of voluntary disclosure for fear of adverse consequences. There is some comfort in the Memorandum's language that notes, "timely voluntary disclosures do not simply reveal misconduct at a corporation; they can also reflect that a corporation is appropriately working to detect misconduct and takes seriously its responsibility to instill and act upon a culture of

[12] Id.
[13] Id.
[14] Monaco Sept. 2022 Mem. at 11.

compliance."[15] However, DOJ likely will have to bolster its assurances with publicly-verifiable examples of specific corporate enforcement actions to ease such concerns—something that DAG Monaco acknowledged in her speech when she stated, "I expect that resolutions over the next few months will reaffirm how much better companies fare when they come forward and self-disclose."[16]

Thus, the timing of disclosure can implicate ethical considerations as counsel advises a company whether, and when, to voluntarily disclose potential misconduct. The Antitrust Division's Leniency Policy states only that a corporation must, "upon its discovery of the illegal activity, promptly report[]" the conduct to the Division in order to qualify for leniency.[17] The Leniency Policy does not define "prompt" timing of disclosure other than to distinguish Type A leniency from Type B leniency as applying to situations in which the Division has not yet received information about the illegal conduct from another source.[18] Nor has the Antitrust Division issued guidance interpreting the Monaco Memorandum's "timely disclosure" requirement for companies to receive full cooperation credit where they do not win the race to obtain leniency.

By contrast, the Criminal Division has issued recent guidance regarding timeliness of self-disclosures. That guidance heightens the timing requirements in the presence of aggravating circumstances or recidivism to near immediate disclosure of allegations of misconduct—even before the corporation may have the opportunity to investigate the allegations in order to determine their credibility.

For companies whose conduct may straddle multiple DOJ divisions, outside counsel advising them regarding whether, and when, to report the alleged misconduct must consider all relevant DOJ policies and guidance – even where it may be unclear and inconsistent. Despite DAG Monaco's strong encouragement to corporations to voluntarily self-disclose, the decision for a company to do is complex and potentially fraught with many collateral consequences.

B. Offering Individuals up for DOJ Scrutiny

While corporations must disclose all relevant information about all individuals responsible for or involved in corporate misconduct in order to obtain full cooperation credit, the possibility exists that corporations will offer up information that could be used to prosecute their executives in order to obtain a more favorable resolution for the company. As such, the Memorandum guidance could impact "common interest" cooperation between corporate and individual counsel and raise questions about the appropriateness, scope, or viability of indemnification agreements under which corporations provide individual legal counsel to their employees. In addition, the DOJ and U.S. Securities and Exchange Commission's coordinated effort to make compensation claw back a de facto requirement for full remediation has the potential of putting individuals and corporation at even greater odds.

[15] Monaco Sept. 2022 Mem. at 6.
[16] Monaco Sept. 2022 Remarks.
[17] U.S. Dept. of Just., Just. Manual §7-3.300 (June 2022).
[18] Id.

C. What to do When Evidence Implicates Officers, Directors, Legal or Compliance?

DOJ's focus on prosecuting individuals strengthens the imperative for any company conducting an internal investigation into potential antitrust wrongdoing to identify those individuals responsible—by commission or knowing omission. Companies will want to reevaluate their compliance policies in light of the Monaco Memorandum's admonition to address employee incentives for good conduct and discipline, including compensation clawbacks, for bad conduct. For outside counsel engaged to lead internal investigations, matters can become especially fraught with issues when the facts suggest that the client's officers, directors, senior management, internal legal counsel, or compliance personnel (who may have hired or directed the outside counsel) engaged in bad acts or permitted them to occur. Similarly, an investigation may raise potential exposure for individual members of a board of directors, which often bears oversight responsibility for the investigation. How outside counsel deals with these challenges is increasingly significant for the integrity of investigations and any cooperation with authorities. Planning, establishing ground rules and lines of communication, and adhering to them will help outside counsel to avoid unnecessary complications.

Below are some hypotheticals to assist in navigating these ethical issues.

Hypothetical: The Individual Directing Your Investigation Is Implicated

During the investigation, a situation may arise in which you, as outside counsel, suspect that the individual directing your investigation, such as the general counsel, Chief Executive Officer ("CEO"), or Chief Compliance Officer ("CCO"), may have been involved in the wrongdoing. If this occurs, you must escalate this information up your established reporting line. Ideally, you have conducted the investigation in a way that maintains its integrity and independence, even if the individual to whom you have been reporting, is potentially implicated.

However, it is important to evaluate whether, at this stage, you need to step out of the investigation as outside counsel because your individual objectivity is compromised. To help make this decision, consider:

- Have you personally developed a loyalty to the individual that may influence your ability to be objective in the investigation?
- Does the individual account for significant other business to your practice or to the firm?

If you determine that you can stay in the investigation, consider whether the integrity of your investigation has been compromised by the individual's prior involvement in or direction of the investigation. To help determine whether reevaluation of or changes to the investigation work plan are warranted, consider:

- Was the individual substantively engaged in the investigation scoping?
- Did the individual direct any portion of the investigation?

Is it possible that the individual otherwise influenced the investigation, such as by directing or intimidating interviewees or interfering with data collection or analysis? Once you have evaluated these points, communicate a strategy to your client for completing the investigation (and reporting on its findings) without the involvement of the implicated party. Your revised strategy may include:

- Establishing a new reporting structure for the investigation;
- Re-scoping parts of the investigation in light of the individual's involvement in scoping decisions in order to ensure that you are adequately investigating all relevant information;
- Analyzing parts of the investigation in which the individual may have been involved to determine what, if anything, needs to be re-examined;
- Assisting the company in procuring individual counsel for the general counsel; or

Hypothetical: Representation of a Company's Board of Directors

A twist on the above-described scenario may occur if a company's board of directors, rather than a company, engages you as outside counsel to advise it in connection with a company's internal investigation, which another outside counsel is leading on a day-to-day basis. In such a situation, complications can arise when, for example, a company's internal investigation reveals that members of the board may have been aware of the alleged criminal antitrust conduct or even have authorized it. A board member may even go so far as to approach you as outside counsel, requesting legal advice as to their potential liability.

As counsel for the board as a whole, you should carefully consider the following when a board member's conduct may be implicated, particularly when a board member seeks your legal advice as to their potential personal exposure:

- Emphasize your obligations to the board. Just as when you represent a company, maintaining clarity on your client relationship is key. When representing a board, it is particularly important that individual board members understand that you are not their personal attorney and that issues they raise individually may be relevant to the board as a whole.[19] If a board member approaches you to discuss their own potential liability, you should remind the board member that because you represent the board (not the board member personally), you cannot agree to keep their secrets. In fact, you may need to report your conversation to the whole company board. You also cannot offer advice as to the board member's personal liability. Model Rule 1.13 requires that you obtain permission from the board before you agree to represent one of its constituents because doing so may well create a conflict with your representation of the board.[20] If you find yourself in such a conflict, the implicated board member may be able to prevent you from disclosing their secrets and you may thus have to withdraw from your representation of the board—forcing it to find new counsel because of your failure to draw clear lines.

[19] Model Rules of Pro. Conduct r. 1.13 (Am. Bar Ass'n 1983)
[20] Model Rules of Pro. Conduct r. 1.13(g) (Am. Bar Ass'n 1983).

- **Advise on process.** Although you cannot advise an individual on a particular personal issue, it may be helpful to advise both the individual and the board as a whole on the best practices for the board to apply in order to address issues related to conflicts and personal legal representation. Advising on process can help all members of a board, without you representing any particular individual or creating a conflict in your representation.

- **Have a plan for referral to individual counsel.** The only advice that you can give a board member who asks you for legal advice is to suggest that the board member consult a lawyer.[21] However, you are not obligated to direct every employee that has a conflict with the board to retain a personal attorney. When advising an individual to seek personal representation, it is useful to have the names of reputable attorneys with relevant experience to recommend on hand. Also, you should familiarize yourself with a company's indemnification policy, as questions about whether the company or the board will pay for such representation often arise. You should also make sure that you are aware of a company's policies that may mandate an employee's cooperation, on pain of discipline if the employee refuses—which may be in tension with the advice of the individual's attorney. If a board member or an employee retains counsel, keep in mind your obligations in communicating with represented parties, which may require you to speak to the attorney rather than the individual.[22]

- **Be mindful of your obligations to U.S. agencies and opposing parties.** It is in your client's interest to be as transparent as possible with all parties regarding your—and its—disclosure obligations. If your client, in this case the board, decides that it does not want to disclose information that you believe needs to be disclosed, you may face additional ethical issues. With DOJ, your ethical obligation of "candor toward the tribunal" may create a conflict between your client's instructions and your ethical obligations.[23] Similarly, you cannot make material misstatements of law or fact to the DOJ, despite your client's inclinations.[24] This can be avoided by ensuring that the person or persons from whom you take direction understands not only the obligation of candor, but also the value and the necessity of it.

- **Recognize board member duties.** Ensure that board members are aware of their duties of care and loyalty. Communicate to the board that each member should exercise reasonable care in their responsibilities on the board and that they should be faithful to the company.

- **Engage with company counsel.** Establish and maintain lines of communication with investigative counsel. As in all matters, having complete and up-to-date information on the status of the investigation is needed to enable you to best represent your client, in this case the board, and assist it in fulfilling its obligations to a company.

[21] Id. at r. 1.13 and cmt. 10.
[22] Id. at r. 4.2.
[23] Model Rules of Pro. Conduct r. 3.3(a)(3) (Am. Bar Ass'n 1983).
[24] Id. at r. 3.4.

D. Other Ethical Issues to Consider in Internal Antitrust Investigations

1. Identification of the Client and Establishment of Clear Reporting Lines

Aside from the ethical issues implicated by the Monaco Memorandum, outside counsel conducting an internal antitrust investigation should consider other general ethical issues that can arise from the outset of an investigation. First, outside counsel should clearly identify your client and your reporting line as outside counsel. Do the following at the inception of your engagement:

- **Clearly identify the client.** In your engagement letter and throughout your discussions with company employees, be clear about who your client is and who it is not. It is essential to make clear to individuals with whom you interact that you represent only the company (or, as the case may be, the board of directors) as an entity and not any individual. Be careful not to treat your in-house contact as your client, rather than as your client's representative. If there is separate outside counsel for the board of directors or a board committee, clearly communicate with that counsel regarding the delineation of responsibilities. If the board of directors is ultimately overseeing your investigation, clarify how this will be done, including reporting lines and the board's involvement in investigation decisions. A clear understanding of your client will help if an executive or other employee seeks your legal advice for personal reasons or tries to assert that you cannot reveal statements that he or she made to you because you had an obligation to them personally.

- **Set expectations of independence.** To preserve the integrity and value of your external presence, set expectations of independence and consistently adhere to and seek to secure the client's adherence to those expectations. This can be done through a variety of ways, including the following:

  - Setting boundaries for involvement in the investigation. It may be advisable to limit the involvement of in-house personnel in data collection and review. Likewise, consider if in-house personnel should be present for interviews of their colleagues and others. The American Bar Association (ABA) Model Rules of Professional Conduct state that a lawyer shall "keep the client reasonably informed about the status of the matter."[25] Significantly, the Model Rules provide that the client can dictate the objectives of an engagement, but the lawyer is responsible for the "means."[26] The Model Rules do not require an attorney to include a representative of the client in the conduct of an investigation itself. It is important to understand the ethical rules that apply in the state or jurisdiction in which you are conducting your investigation.

  - Leading the direction of the investigation. If in-house personnel suggest a particular direction for the investigation, take it under advisement, but do not let it control your actions. The ABA Model Rules state that an attorney should "reasonably consult with the client about the means by which the client's objectives are to be accomplished" but do not require an attorney to let the client lead the investigation.[27] By

[25] Model Rules of Pro. Conduct r. 1.4(a)(3) (Am. Bar Ass'n 1983).
[26] Id. at 1.4(a)(2).
[27] Id.

owning the investigation, you as outside counsel will help preserve the investigation's integrity in the event in-house personnel with whom you may have interacted are implicated in the investigation.

- **Establish reporting lines.** Establish at least two lines of potential reporting. In some scenarios, day-to-day reporting (the "solid line" reporting) may be with the general counsel. However, at the outset of the investigation, outside counsel should establish "dotted-line" reporting to another party, such as a company's board of directors, a committee of the board, an independent director, the chair of the board's audit committee, or the chief compliance officer. Such reporting lines need not be formal and can oftentimes be informally established, but they are critical in ensuring proper corporate oversight of the investigation. Keep in mind that with allegations of recent wrongdoing, there may be widespread involvement by current company employees, management, and board members.

2. Additional Ethical Considerations Related to Investigations Procedure

There are also additional ethical considerations related to the logistics and procedure of the investigation to consider. As you conduct a scoping exercise, collect and review documents, and conduct substantive interviews, consider the following:

- **Third party management of forensic data collection.** Unless a company is required by law to disclose collection or analysis of third party data holders, consider whether you can collect data without informing the custodians whose data you would like to collect. A best practice in the United States is to back up employee data and suspend regularly schedule document purges *prior* to disclosing the existence of the investigation during scoping interviews or issuing a written document hold notice. Doing so will make it more difficult for employees at a company to tamper with the data and will also make it more difficult for those who may be potentially involved in the alleged wrongdoing to see the data that you have collected. It may also be best to use a third-party vendor to collect data from the company (rather than relying on a company to collect and transmit the data to you).

- **Data privacy considerations.** The Monaco Memorandum's new policy discouraging the use of personal devices and third-party data platforms for work means that companies should reevaluate their data privacy policies up front. In the event of an investigation, companies most likely will need to collect data from their employees' personal devices in order to show cooperation. While U.S. employees are typically in employment-at-will arrangements, be sure to consult with local counsel when conducting global investigations. Also, consider whether a "give-me-your-phone-or-you-are-fired" approach is in the best interest of the corporate client. If a corporation is too heavy handed, it may jeopardize its ability to produce individuals for witness interviews to the DOJ—a key factor in assessing cooperation. Be sure that contract and junior attorneys are absolutely clear that personal data collected in the course of an investigation is to be kept confidential. Professionalism, in addition to ethical ad privacy considerations, dictates that only relevant data on personal devices be discussed.

- **Confidentiality in interviews.** Consider maintaining utmost confidentiality surrounding interviews. In addition to asking interviewees not to discuss their interviews with others to the extent possible, work to ensure that the very fact of each interview is confidential. This confidentiality will help interviewees not feel or be pressured to withhold information or mislead the investigation. If a company or country has strong antiretaliation policies or laws, you may also reassure the interviewee that they will operate in their favor in order to encourage candor—but do not do so if there is not a reasonable expectation that this will be the case. It is best if anyone who may be implicated in the investigation, regardless of their position (and including management), not know who your interviewees are. You may want to conduct interviews off site if there are no appropriately private places at the client's office for the interviews. If the client is located in a country with widespread fears of surveillance, consider bringing sensitive employees out of the country. Additionally, consider whether having in-house personnel present in interviews may chill discussion.

- **Timing.** Time is of the essence. Once a document hold notice is issued and interviews begin, the fact that an investigation is ongoing becomes known, and there is only a finite time during which you may reasonably rely on confidentiality being maintained. Gathering the necessary documents and conducting interviews of important witnesses within this window is important to maintaining the integrity of the investigation. Where possible, sequence and prioritize investigative steps to ensure that key data and witnesses can be reached reasonably promptly after the fact of the investigation becomes known.

III. CONCLUSION

DOJ's increased emphasis on self-disclosure, cooperation, and holding individuals accountable for corporate wrongdoing adds a layer of complexity to the actions of outside counsel navigating representations of companies and boards in internal investigations.

In particular, outside counsel may encounter a variety of ethical issues, including:

- Managing individual interests of employees and board members while balancing and fulfilling obligations to the client entity.

- Maintaining the integrity of an investigation, including when this means having to reevaluate scope, adjust reporting lines, or even step aside.

- Dynamics in interacting with other counsel and represented individuals.

Foresight and planning for these potential ethical issues can help counsel react quickly and seamlessly to complicating factors as they arise during an internal investigation, notably the uncovering of evidence that could implicate a company's general counsel or board of directors in the alleged wrongdoing.

THE NECESSITY TO SCREEN YOUR BUSINESS PARTNERS

And the challenges that come with it

Laura Louca

AUTHOR

Dr. Laura Louca is a lawyer at the lawfirm BLOMSTEIN and she specializes in European and German foreign trade law. She regularly advises clients on export control law issues and infringements, in particular on the export of goods and technology under the Dual-Use Regulation, the German Export and War Weapons List, as well as on EU sanctions law. She represents German and international clients both vis-à-vis the European Commission and the Customs Administration, the Federal Office for Economic Affairs and Export Control (BAFA), federal ministries as well as before administrative and fiscal courts.

She also advises clients on trade compliance programs relating to sanctions and export control laws. She has significant experience in accompanying internal and external investigations and self-disclosures in cases of breaches of foreign trade law, closely collaborating with the competent authorities if necessary.

TABLE OF CONTENTS

I. INTRODUCTION

Restrictive measures in the form of sanctions are a common tool of the western world's security policy to affect change in the conduct or policy of those targeted. The US has been using these measures targeting all sorts of countries, groups and sectors, while often obligating not only US persons but also non-US persons to follow them. While EU sanctions have rarely been as comprehensive as US sanctions, targeting persons or group of persons has always been a way to limit the targeted persons capabilities to continue its condemnable actions.

One of the most common restrictive measures is the freezing of assets and the prohibition from making funds and economic resources available to certain listed persons. While larger companies especially have been aware of such restrictions and have tried implementing the necessary measures into their daily business, many questions still remain. What exactly does "funds and economic resources" mean? Can I screen my business partners manually? Do I need to screen their parent companies? Won´t the bank do this anyway? And most important, what happens if I violate the sanctions regulations?

The Russian invasion into the Ukraine has brought a new wave, or, should I say, several new waves of sanctions which pose new challenges for economic operators. At the same time, a sanctioned country has rarely had as many economic ties to Europe as Russia. Therefore, knowing one's own due diligence obligations is more important than ever. The following article will outline the legal framework in connection with the prohibition on the provision of funds and economic resources and the resulting due diligence requirements, and will give a guideline which aims to help in the day-to-day business. While the point of reference are EU sanctions regulations, the same or similar principles apply in most jurisdictions, such as the US or the UK. In an attempt to ensure the attention of every reader, I will start by answering the last question first:

II. PENALTIES FOR SANCTIONS REGULATIONS

The penalties of sanctions violations differ in the different jurisdictions. For example, in Germany, violations of sanctions regulations can constitute a misdemeanor (in the case of negligence) or in some cases even a criminal offense (in the case of intent). The U.S. authority OFAC treats violations as a serious threat to national security and foreign relations. In both jurisdictions violations are thus punishable with imprisonment and high fines for all natural persons and entities involved in the violation. I dare say that, while the intensity of the punishment can severely differ between the different legislations, law enforcement authorities now more than ever have one thing in common. It seems that they finally all agree that violations are not to be taken lightly.

In addition to these penalties, companies must fear other grave consequences, such as freezing of the company´s own accounts or assets, reputational damage, loss of permits or privileged statuses (such as the status of an Authorized Economic Operator) or even the exclusion from future tenders.

III. THE PROHIBITION TO PROVIDE FUNDS AND ECONOMIC RESOURCES

Once in force, the prohibition to provide funds and economic resources overrides all incompatible contractual arrangements. Thus, regulations apply notwithstanding any rights conferred by or obligations provided for in any contract that entered into force prior to the regulations and preclude the completion of acts which implement such contracts.

The prohibition on making funds or economic resources available prohibits the direct or indirect provision of funds or economic resources to persons listed in the corresponding regulation. Such prohibitions can be found in most recent sanctions regulations, such as Article 2 (2) of Regulation (EU) No. 269/2014 (Russia). The German Federal Court of Justice has stated that an indirect provision exists, "*if economic resources are supplied to non-listed third parties who are willing to pass them on to the listed persons or organizations*".[1] This willingness is presumed in the case of existing ownership of the company or in the case of a controlling position of the listed person. According to the EU Commission's guidance, a provision to a company that is majority-owned (i.e. more than 50%) or otherwise controlled by a listed person is generally deemed to be an indirect provision to the listed person.

While direct or indirect shareholdings of more than 50% in the company concerned are decisive for the characteristic of ownership, a controlling position is less clear-cut. The EU Commission has established several exemplary criteria for this purpose, the fulfillment of which generally leads to the assumption of control:

> (a) having the right or exercising the power to appoint or remove a majority of the members of the administrative, management or supervisory body of such legal person or entity;
>
> (b) having appointed solely as a result of the exercise of one's voting rights a majority of the members of the administrative, management or supervisory bodies of a legal person or entity who have held office during the present and previous financial year;
>
> (c) controlling alone, pursuant to an agreement with other shareholders in or members of a legal person or entity, a majority of shareholders' or members' voting rights in that legal person or entity;
>
> (d) having the right to exercise a dominant influence over a legal person or entity, pursuant to an agreement entered into with that legal person or entity, or to a provision in its Memorandum or Articles of Association, where the law governing that legal person or entity permits its being subject to such agreement or provision;
>
> (e) having the power to exercise the right to exercise a dominant influence referred to in point without being the holder of that right;
>
> (f) having the right to use all or part of the assets of a legal person or entity;
>
> (g) managing the business of a legal person or entity on a unified basis, while publishing consolidated accounts;

[1] BGH, decision of 23 April 2010 – AK 2/10, para. 20, free translation.

(h) sharing jointly and severally the financial liabilities of a legal person or entity, or guaranteeing them.[2]

As these are just examples of cases in which the EU Commission assumes control, individual corporate structures, agreements or rules of the Articles of Association may justify a case-by-case examination.

Funds include financial assets and economic benefits of any kind, including, but not restricted to, cash money, cheques, monetary claims, drafts, money orders, and other instruments of payment, deposits with financial institutions or other entities. Economic resources are financial assets of any kind, irrespective of whether they are tangible or intangible, movable or immovable, that do not constitute funds or means to acquire them. Making funds or economic resources available to a designated person or entity, be it by way of payment for goods and services, as a donation, in order to return funds previously held under a contractual arrangement, or otherwise, would be a violation of the prohibition.

IV. DUE DILIGENCE

Every company that has to deal with such sanctions needs a structured plan of action so as not to overlook any necessary steps and end up facing accusations of negligence or even intent. This includes a clear understanding of the necessary due diligence requirements. While the guidelines of the EU Commission might have the purpose of helping entities understand the legal requirements better and navigating their compliance duties, the main question remains unanswered: to what extent must companies screen their business partners and how much effort do they need to put in to uncover the ownership and control relationships of their direct and indirect business partners? First, the necessity to screen applies to all companies, regardless of their size and form. Second, companies must not only screen their suppliers or intermediaries but also their customers and in some cases also their internal or external employees. This means that several departments and individuals could be jointly responsible. Third, the question of how much a company must investigate the ownership and control of its business partner has not yet been conclusively clarified. The EU Commission has not issued any guidance on this, partly because it always emphasizes that the requirements may vary from case to case. However, this question is important because violations of the prohibition can constitute an administrative or even a criminal offense. Even if a company acts negligent, the monetary penalties can reach very high figures, depending on the jurisdiction.

The standard of negligence is linked to the care required in the situation. This is also clear from the regulations themselves. For example, Art. 10 (2) of Regulation No. 269/2014 states that:

> "*Actions by natural or legal persons, entities or bodies shall not give rise to any liability of any kind on their part if they did not know, and had no reasonable cause to suspect, that their actions would infringe the measures set out in this Regulation*."

Thus, an allegation of negligence can only be made if there were reasonable grounds to believe that a sanction would be violated. This also applies to criminal and administrative offences law, as the ECJ has made clear in the context of the Iran embargo

[2] EU, Best Practices, 4. Mai 2018, Rn. 63.

> „*Secondly, it is necessary to point out that Article 12(2) of Regulation No 423/2007 exonerates from all liability 'of any kind', including, accordingly, criminal liability, persons who did not know, and had no reasonable cause to suspect, that their actions would infringe the prohibition on making available an economic resource laid down in Article 7(3) of that regulation*".[3]

Against this background, the requirements for due diligence must not be overstretched and are, moreover, dependent on the respective economic operators concerned. Considering the large amount of payment transactions, some argue that

> "*It is unreasonable to expect them [i.e., the employees in charge] to conduct their own further inquiries; rather, they can rely on the information available to them. In the problematic cases of indirect provision, an employee who knows nothing about the background of the attribution to a listed entity cannot foresee that with his release of a payment - indirectly - a listed entity is also benefited*".[4]

Even if these arguments cannot be generalized, reasonability sets a limit to the legal requirements. Therefore, negligence can only be assumed if the acting party could have foreseen the prohibited provision to a sanctioned person according to his knowledge and abilities. Accordingly, the following indications could be used as a guide:

- The most common misconception regarding the screening obligations is that the bank will take over the screening once a payment has been initiated, thus releasing economic operators from their obligations. Indeed, banks do their own screening. However, the purpose of this screening is to meet their own responsibilities and not the responsibilities of economic operators. They are neither agents nor service providers or representatives in this regard. In the contrary, once a bank has detected such an attempted payment, they can inform the prosecuting authorities.

- Business partners with links to sanctioned countries should be screened by using a screening program. While a company can also use publicly available sources, such as the EU Sanctions Map, the effectiveness of such depends on several factors. First, depending on the amount of business partners, such a manual screening can last too long and will probably not keep up with rapid changing sanctions listings. Additionally, even if you can effectively screen your direct business partner, publicly available tools such as the EU Sanctions Map will most likely not provide any information on the shareholders and ultimate beneficial owners. Therefore, there is still a risk of violating the sanctions regulations by providing funds or economic resources to a party that is owned or controlled by another sanctioned person. Surely, it is not impossible to do this research based on other publicly available sources, such as the media, the commercial register and so on. However, the amount of effort that would have to be put into this is probably much higher. At the same time, unless the company has experts in the field, the reliability of such kind of research is limited. If

[3] ECJ, Judgement from 21. Dezember 2011 - C-72/11, para. 55, emphasis added.

[4] Prof. Dr. Wolfgang Spoerr/Dr. Tilmann Gäde, *Strafrechtliche Verantwortlichkeit von Compliance-Mitarbeitern von Banken und Zahlungsdienstleistern bei der Abwicklung und Kontrolle von Zahlungsverkehr*, CCZ, 77, 82 (2016), free translation.

companies do not want to use a screening tool themselves, they can outsource the screening to an adequate service provider.

- With regard to natural persons, the information should aim to include, in particular, surname and first name (where available also in the original language). Aliases, sex, date and place of birth, nationality, address, identification, or passport number can be used additionally to confirm the identity of a potential screening match. With regard to entities, the information should aim to include in particular the full name, principal place of business, place of registration of office, date and number of registrations.

- The question of whether the screening should take place prior to concluding a contract or after, but prior to providing any funds or economic resources, has always been part of several debates. In the absence of clear case law and the tendency of a wide interpretation of the sanctions regulations by the authorities, sanctions law experts recommend to screen the business partner prior to concluding a contract. The sanctions regulations prohibit any (direct or indirect) provision of economic resources, including assets of any kind. Contractual claims will usually not be able to be denied a certain economic value, so that the risk of a violation remains. An early screening is especially important when taking other regulations, which prohibit all transactions of any kind with certain listed persons, into account.

- Information obtained by screening or by other means must not be ignored. Neither should obvious indications regarding such matters. If there are indications that suggest that sanctioned persons are in a position of ownership or control, the requirements for personal due diligence increase and justify an obligation to investigate.

- This in turn must be met within the bounds of reasonableness. In this context, it would appear reasonable to conduct more in-depth research in publicly accessible sources of information, to recall upon any insider knowledge from the market, and to make inquiries with the (potential) business partners concerned. Once the existing doubts have been clarified and there are no further indications that the business partner could be indirectly sanctioned, an accusation of negligence can generally be ruled out, even if an infringement would later be determined.

- The audit process should always be well documented.

- With regard to the screening of other participants in the supply chain, there are again no specific requirements regarding this specific provision. Here, too, it is important not to ignore existing indications, and to screen known (end) customers of one's own contractual partners, - especially if there are doubts and reasons to believe that they will finally receive the provided economic resources. However, the limit of reasonableness does not require the company to track the (non-listed) goods concerned across several levels of the supply chain. In case of doubt, an end-user declaration could be required from the contractual partner in order to show that the company has done everything reasonable to exclude a transfer of the goods to sanctioned persons.
- Even if an ownership or control position of listed persons is to be assumed, the described presumption that a provision to the non-listed held or controlled company is deemed to be

an indirect provision to the sanctioned person can be rebutted in individual cases. The previous practice of the authorities in this regard are outdated. As is stated in the EU Best Practices Paper, the presumption does not apply if "*it can be reasonably established on a case-by-case basis, using a risk-based approach and taking into account all of the relevant circumstances [...] that the funds or economic resources concerned will not be used by or for the benefit of the listed person or entity*".[5] In this regard, several criteria are taken into account, such as the date and nature of the contractual links between the organizations concerned or the characteristics of the funds or economic resources provided, including their possible practical use by a designated organization and the ease of transfer.[6]

- Overall, the demands on companies have increased as sanctions lists have multiplied in recent years. Particularly when business relations have a nexus to targeted countries, economic operators must exercise a special degree of caution. When in doubt, companies should consult with the authorities or legal professionals. When in doubt, companies should not ignore obvious signs and proceed with the transaction.

[5] EU Best Practices, 4 May 2018, para. 66.

[6] EU Best Practices, 4 May 2018, para. 66.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

HOW TO IMPLEMENT AN EFFECTIVE CRIMINAL COMPLIANCE MANAGEMENT SYSTEM

Elias Schönborn & Robert Keimelmayr

AUTHOR

Dr. Elias Schönborn is an Attorney at law at DORDA Rechtsanwälte GmbH and specialized in criminal compliance, white-collar crime, internal investigations and civil procedure law.

Mag. Robert Keimelmayr is Associate at DORDA Rechtsanwälte GmbH and specialized in white collar crime, civil procedure law and arbitration.

ABSTRACT

As the number of government investigations in the corporate and public sectors increases worldwide, the interest in implementing effective internal rules to avoid non-compliance with the law and its many negative consequences is growing. In this context, one may think primarily of the general concept of Compliance, without considering its various forms in different areas of law. In particular, Compliance with regard to criminal law - also referred to as 'Criminal Compliance' – has received greater attention in recent years. What applies in general to Compliance is particularly true for Criminal Compliance: Only a Compliance Management System tailored to the individual company can effectively prevent criminal offences.

TABLE OF CONTENTS

I. CRIMINAL COMPLIANCE AND ITS OBJECTIVES

In a nutshell, Criminal Compliance - as indicated by its name - primarily deals with the prevention of criminal law violations.[1] Companies usually strive to avoid criminal law offences and its associated risks and disadvantages. Consequently, Criminal Compliance aims to provide an additional 'layer of protection' for companies and public institutions to prevent criminal conduct as far as possible and to proactively address existing and potential future non-compliance with criminal law provisions.[2]

The benefits of Criminal Compliance are striking: In a global comparison, companies that have implemented written compliance guidelines suffer on average approx 40% less financial damage from white-collar crime than companies which have not established comparable measures.[3] Effective compliance tools also significantly reduce the risk that managers, board members, employees, compliance officers or the company itself will be prosecuted. In addition, also business partners can rely on a solid and trustworthy business relationship, which of course also brings competitive advantages for the company.[4] In the case of pending criminal proceedings in particular, compliance measures can also have a positive impact on the likelihood of an acquittal, withdrawal of prosecution or reduction of an impending fine.

In summary, the potential benefits of effective Criminal Compliance are considerable. So what can companies do to implement, customize, and fine-tune their criminal law compliance efforts?

II. CRIMINAL LAW COMPLIANCE MANAGEMENT SYSTEMS

In general, the entirety of all compliance regulations, measures and principles of conduct that a company implements to comply with the law is called 'Compliance Management System' (CMS).[5] The individual design of a CMS and the corresponding question which measures and instruments may be implemented mainly depends on the respective company's geographical location, type, size and organizational structure.[6] However, most CMSs are based on the same components derived from various existing laws and international standards.

A. Development of Criminal Law Compliance Management Systems

In fact, some essential standard elements have emerged which serve as general guidelines when it comes to implementing an efficient CMS – this is especially true when it comes to criminal law.[7] These

[1] Cf *Soyer/Pollak* in *Kert/Kodek (Eds.)*, Das große Handbuch Wirtschaftsstrafrecht[2] (2022), mn 28.6.

[2] Cf *Soyer/Pollak* in *Kert/Kodek (Eds.)*, Das große Handbuch Wirtschaftsstrafrecht[2] (2022), mn 28.8.

[3] *ACFE*, Occupational Fraud 2022: A Report to the Nations, 34 et seqq; available at: https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf.

[4] Cf *Darakhchan/Freiler-Waldburger* in *Sartor (Ed.)*, Praxisleitfaden Compliance ², p 31.

[5] Cf *Soyer/Pollak* in *Kert/Kodek (Eds.)*, Das große Handbuch Wirtschaftsstrafrecht[2] (2022), mn 28.9.

[6] Cf *Veit*, Compliance und interne Ermittlungen (2021), mn 179.

[7] Cf *Morawetz/Sartor/Schwab* in *Sartor (Ed.)*, Praxisleitfaden Compliance ², p 10.

standard elements are based on various rules and standards of which the following are worth mentioning[8]:

First and foremost, the UK Bribery Act 2010 contains most of the elements of a typical CMS. This UK norm aims at preventing corruption and, accordingly, sets out six principles for organizing companies in this respect, i.e. proportionate procedures, top-level commitment, risk assessment, due diligence, communication (including training) as well as monitoring and reviewing.

In addition, the development of the essential components of a Compliance Management System (CMS) has been significantly influenced by the US Foreign Corrupt Practices Act (FCPA). This act prohibits any US individual or entity from giving, offering, or committing to give money to any foreign official in exchange for business retention or acquisition, and has laid a strong foundation for the establishment of a CMS. Moreover, the FCPA applies to non-US individuals and companies who, directly or through intermediaries, cause corrupt payments to be made within the United States. The scope of the FCPA in the international context is very wide.

What's more, also the International Organization for Standardization has published the international ISO standard DIN ISO 37301:2021 which describes in detail the criteria for an effective CMS. It provides parameters and guidance for the implementation, adjustment, evaluation and improvement of Compliance Management Systems. In summary, this standard covers all the relevant topics such as assessment of compliance risks, training of employees, a complaints system and provisions for conducting internal investigations. As usual, the ISO standard provides the option of certifying an implemented CMS if all the criteria are met.

Furthermore, ISO 37001 is an international standard that provides requirements and guidance for organizations to establish, implement, maintain and improve an effective anti-bribery management system (ABMS). The standard is designed to help organizations prevent, detect and respond to bribery-related risks and incidents. Key requirements include a clear anti-bribery policy, management commitment, regular risk assessments, due diligence of business partners, effective communication and training, and financial and non-financial controls. The standard requires regular internal audits and external audits by accredited certification bodies to ensure compliance. ISO 37001 certification can enhance an organization's reputation, particularly with stakeholders who value ethical behaviour and good governance.

In Austria, the possibility of corporate criminal liability under the Corporate Liability Act of 2006 (Verbandsverantwortlichkeitsgesetz) has provided an indirect incentive (through fines towards companies) for the introduction of a compliance system based on criminal law. Many other countries have comparable laws.

Spain, for example, has gone one step further: The Spanish Standards Association has published UNE 19601, a standard that establishes various requirements for the implementation of Criminal Compliance Management Systems, with a focus on reducing criminal risks in companies. This standard is in

[8] Cf *Veit*, Compliance und interne Ermittlungen (2021), mn 182 et seqq.

line with other international standards and aligned with the Spanish Criminal Code, which means it can be taken into account in Spanish legal proceedings.[9]

Essentially all (Criminal) Compliance Management Systems contain three main components: **Prevention**, **Cognition** and **Reaction**.[10] Although companies tend to focus primarily on Prevention, i.e. on the avoidance of violations and criminal offenses,[11] the other components are essential for a frictionless and effective CMS. Following, these key points for the implementation and customization of a functioning Criminal Compliance Management System shall be addressed in the following.

B. Prevention

The most fundamental component Prevention can be broken down into various sub-areas, each focused on different principles:

1. Compliance Risk Analysis

In order to establish a basic understanding for all relevant compliance measures, it is necessary to identify the most virulent risks for a company as part of a so-called Compliance Risk Analysis.[12] The risks are determined on the basis of various company related factors,[13] such as the company's sales model, customer structure, characteristics of the business activities as well as violations of standards and criminal offences in the past. Workshops, interviews with individual employees or questionnaires are particularly suitable for risk identification, and all levels of the company should be involved. The aim of the Compliance Risk Analysis is to provide a comprehensive overview of potential threats and problems in the respective company. To ensure that the established risk analysis remains up to date and in particular reflects ongoing internal and external developments, it is advisable to update it every one to two years.

Companies need to be aware of a wide range of criminal law risks. Of particular relevance to the business sector are, for example, risks related to embezzlement, fraud, breach of trust, acceptance of gifts by persons in a position of authority, fraudulent or grossly negligent inducement of insolvency, manipulation of balance sheets, money laundering and agreements restricting competition in tender procedures. In addition, corruption offences and the prohibition of abuse of official authority are particularly relevant.

[9] Cf https://www.navarrollimaabogados.com/en/news/compliance-system-managemente-une19601/.

[10] Cf *Kahlenberg/Schäfer/Schieffer*, in *Busch* et al, Antikorruptions-Compliance, p 823; *Krakow/Larcher/Petsche/Zareie* in *Petsche/Mair* (Eds.), Handbuch Compliance[3] (2019), p 239; however, the classification is sometimes rather blurry and some measures affect several areas.

[11] Cf *Soyer/Pollak* in *Kert/Kodek (Eds.)*, Das große Handbuch Wirtschaftsstrafrecht[2] (2022), mn 28.7.

[12] Cf *Koukol,* Compliance and Criminal Law (2016), p 26.

[13] Cf *Kahlenberg/Schäfer/Schieffer* in *Busch* et al, Antikorruptions-Compliance, p 824.

Recommendation:
Typical risk indicators of possible criminal law risks are conflicts of interest, sham contracts and sham invoices, high commission payments, secret side agreements to written contracts, imbalance of performance ratios, kick-back payments, asset transfers despite (impending) insolvency, ineffective control mechanisms or lack of independence of supervisory bodies.[14]

2. Compliance Guidelines

The results of the Risk Analysis form the basis for Criminal Law Compliance Guidelines (also called 'code of conduct', 'compliance policy/manual' etc).[15] The guidelines should be written in plain, easy-to-understand language and as short as possible to allow for smooth implementation in the daily work routine of employees.[16] Depending on the company's business activities, different codes of conduct may be implemented, focusing for example on the avoidance of conflicts of interest and financial crimes, anti-corruption, proper dealings with public officials and lobbying, as well as rules on gifts, invitations and other benefits.

3. Corporate Communication

Another essential prerequisite for any CMS is the establishment of an internal compliance culture.[17] This requires a shared and internalized 'compliance mindset' throughout the organization. In order to accomplish such mindset, it is primarily the task of the company's management and its executives to reinforce and affirm compliance with the Compliance Guidelines vis-à-vis the rest of the employees ('Tone from the Top').[18]

In addition to this Tone from the Top, attention should also be paid to the 'Tone from the Middle'. The latter refers to the fact that middle management should also address and enforce criminal law compliance within the company. The reason for this is that mid-level managers are usually in direct and daily contact with their subordinates and can therefore exert a greater influence on employees' compliance with the Code of Conduct.[19]

4. Staff Training

However, Corporate Communication from the company's management levels is usually not sufficient to create a common and mutual understanding of the Compliance Guidelines among all employees.

[14] Cf also *Dann* in *Busch et al*, Antikorruptions-Compliance (2020), p 870 et seqq.
[15] Cf *Kahlenberg/Schäfer/Schieffer* in *Busch* et al, Antikorruptions-Compliance, p 826.
[16] Cf *Veit*, Compliance und interne Ermittlungen (2021), mn 201.
[17] Cf *Veit*, Compliance und interne Ermittlungen (2021), mn 186.
[18] Cf *Koukol*, Compliance und Strafrecht (2016), p 26; *Freiler-Waldburger/Pilecky/Sartor* in *Sartor (Eds.),* Praxisleitfaden Compliance ², p 41.
[19] Cf *Freiler-Waldburger/Pilecky/Sartor* in *Sartor (Eds.),* Praxisleitfaden Compliance ², p 89f.

Therefore, it is advisable to continuously explain the content of implemented compliance rules and its meaning to the staff in the most clear and practical manner as possible.[20]

A structured compliance training program for employees is therefore essential. Depending on the size of the company and its target group, different training courses may be held for managers, department heads, sales, etc. Particularly, in the context of criminal law, it makes sense to train employees on the correct and suitable behavior in case of house searches, which is especially important for management, IT and reception staff as well as members of the legal or compliance department.

C. Cognition

1. Whistleblowing System

Whether the implemented compliance measures ultimately achieve their intended effects and objectives only becomes apparent after they have been in place for a certain period of time. From an empirical point of view, it is usually the staff that first becomes aware of specific violations or gaps in the Compliance Guidelines.[21] In this context, it is important to ensure that whistleblowers are protected when reporting violations and that the issues raised are taken into account when revising and updating compliance policies. It is also worth mentioning the European Whistleblower Directive[22], which establishes minimum whistleblowing standards for companies with at least 50 employees.

2. Internal Investigation and Audits

Another essential element is active investigation relating to possible violations and criminal offenses. Here, a distinction must be made between internal investigations and audits.

Internal investigations are usually only carried out on the basis of specific indications and reports of (possible) violations. Either the company investigates the incident itself or it is assisted by experts. Especially in the case of criminal allegations, it makes sense to (also) involve a criminal law specialist. Audits, on the other hand, are regular or ad hoc reviews that examine not only compliance with the CMS, but also its specific design.[23] Audits can be carried out by internal or external representatives.[24]

Upon completion of an internal investigation or audit, a report is regularly prepared on the facts found. Based on this work, it is advisable to have a legal opinion prepared by an expert, outlining the key findings, legal consequences, risks and obligations.

[20] Cf *Kahlenberg/Schäfer/Schieffer* in *Busch et al*, Antikorruptions-Compliance, p 831; *Veit*, Compliance und interne Ermittlungen (2021), mn 222 et seqq.

[21] Cf also Recital 1 of the Whistleblowing Directive (EU) 2019/1937.

[22] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

[23] Cf *Kahlenberg/Schäfer/Schieffer* in *Busch* et al, Antikorruptions-Compliance, p 836.

[24] Cf *Kahlenberg/Schäfer/Schieffer* in Busch et al, Antikorruptions-Compliance, p 836; *Pasewaldt/Raiser*, in *Busch* et al, Antikorruptions-Compliance, p 908.

Recommendation:
Possible warning signs which indicate illegal behavior with regard to white collar crime are, for example, the destruction, concealment, or falsification of evidence, backdating, missing invoices and receipts, payments close to or just below certain thresholds that trigger a control obligation, incorrect accounting of business transactions and ineffective control mechanisms.

3. Monitoring

Finally, to find out whether and to what extent employees adhere to the Compliance Guidelines, regular Monitoring is required.[25] It can be used to monitor a variety of different factors, such as the effectiveness of employee training, the efficiency in dealing with compliance violations or the timeliness of compliance guidelines.

Usually, specific indicators (so-called 'key performance indicators') are used for Monitoring, e.g. the number of investigations and audits carried out, the sanctions imposed or the training measures implemented.[26] Based on the results of such Monitoring, conclusions may be drawn in respect to the effectiveness of an existing CMS and its potential for improvement ('Lessons Learned').

D. Reaction

Clear consequences and sanctions for misconduct are necessary to ensure that employees adhere to compliance policies.[27] Possible reactions to violations of law or internal Compliance Guidelines are additional training, but also more serious actions under labor law such as a formal warning, transfer or dismissal.[28] In fact, in case of criminal offenses, dismissal will often be the most adequate form of reaction.

III. CONCLUSION

The goal of reducing criminal law risks can only be effectively achieved if a Compliance Management System goes beyond superficial and general objectives and considers the inherent criminal law risks of the respective company as well as new developments. Ultimately, the implementation of an effective CMS remains a case-by-case decision: it requires a detailed risk analysis as well as an in-depth criminal law analysis. Only by continuously adjusting, customizing and adapting can a far-reaching prevention of criminal liability can be achieved.[29] Hence, those entities who implement a Criminal Law Compliance Management System, align it with the existing standards and keep it up to date can successfully minimize their criminal liability.

[25] Cf *Soyer/Pollak* in *Kert/Kodek (Eds.)*, Das große Handbuch Wirtschaftsstrafrecht[2] (2022), mn 28.16.

[26] Cf *Kahlenberg/Schäfer/Schieffer* in *Busch* et al, Antikorruptions-Compliance, p 837.

[27] Cf *Koukol*, Compliance and Criminal Law (2016), p 28.

[28] Cf *Veit*, Compliance und interne Ermittlungen (2021), mn 235.

[29] Cf *Veit*, Compliance und interne Ermittlungen (2021), mn 239 et seqq.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

THE COMPLIANCE OFFICER AND HIS GUARANTOR POSITION

Siegfried Herzog

AUTHOR

Siegfried Herzog holds a doctorate in law and is an entrepreneur in Liechtenstein. He specializes in data protection law, compliance and digitization in the financial sector. Before Siegfried Herzog became self-employed in July 2019, he worked as a lawyer at a Liechtenstein financial group, where he was able to develop and expand his expertise in the fiduciary sector and the associated regulatory framework as well as progressive digitization requirements. Since 2019, Siegfried Herzog has been supporting various domestic and foreign financial intermediaries in the areas of regulation, compliance, data protection law and digitization. A special focus is on Virtual Asset Service Providers (VASP) and new trusted technologies.

TABLE OF CONTENTS

I. INTRODUCTION

The tasks and requirements of a Compliance Officer have changed significantly in recent years. This is no longer exclusively tied to the task of ensuring compliance with rules in companies and preventing illegal activities, but also includes an increasing number of governance obligations and risk management duties for the Compliance Officer. A state-of-the-art Compliance Officer should therefore be deeply rooted in the corporate structure, have proven industry knowledge as well as unlimited access to information and be professionally qualified in order not to have to deal with criminal liability.

II. DEFINITION OF OMISSION

Criminal law fundamentally distinguishes between active action and omission, i.e. doing something versus failing to do something. Criminal law similarly distinguishes between offense by commission and objective crime. When there is an offense by commission, criminal liability is already linked to the performance of a specific act. Realization of such success is not relevant. In contrast, with objective crime, the outcome of the act is more important than the act itself. Objective crime requires that a criminal act be achieved. While a criminal act can be realized by an intentional or negligent act, "qualified idleness"[1], i.e., the failure to perform a required action[2] and thus the omission of a concrete legal obligation to act in certain cases is punishable as well.

III. IS THE COMPLIANCE OFFICER AT RISK?

In principle, it can be assumed that a compliance specialist behaves in accordance with the rules and is not actively involved in illegal activities. However, there's still a risk that, even in the case of rule-keepers, the success of criminal conduct will be recognized for personal reasons or labor law considerations, but this will not be prevented or even turned a blind eye. In such cases, there is no active participation of the compliance specialist. But still the Compliance Officer fails to comply with its function-immanent/legally imposed monitoring and prevention obligation and only allows success to occur through this inaction.

IV. LEGAL PREREQUISITES OF OMISSION

In such cases, § 2 of the Liechtenstein Criminal Code (LCC) must be examined. According to § 2 LCC, criminal liability for omission must be an objective crime according to which the legal system imposes an **obligation to avert success** for the perpetrator, the **fulfilment of which is possible and reasonable** (guarantee) and the omission is **equivalent** to objective crime ("equivalence corrective").

[1] *Hilf*, Wiener Kommentar[2] 59 Lfg., § 2, 1.

[2] *Kienapfel/Höpfel*, Strafrecht AT[16], Z 7, 17.

V. QUALIFYING AS GUARANTOR

While the distinction between activity and success offences has already been described above, an omission can only be punishable according to §2 LCC if the perpetrator has a legally defined obligation to avert success (guarantor). A guarantor within the meaning of §2 LCC is anyone who is legally responsible for ensuring that success does not occur[3]. The following criteria indicate a guarantor position:

i. There must be a legal obligation under the law, from a contractual or contractually similar assumption of obligations or from a previous conduct that creates a risk. Mere moral or moral duties, on the other hand, are not enough.

ii. The legal obligation must apply to the perpetrator in particular, i.e., be limited to a relatively small circle of persons obliged to act. General obligations, which have a general effect, are insufficient.

Consequently, the position as guarantor and the resulting obligation to avert success may arise from both statutory and contractual obligations. However, it is questionable whether and, if so, under what circumstances a Compliance Officer should be regarded as a guarantor. There are no corresponding (published) judgments in Liechtenstein. However, there is a from the German BGH, that is analogous to the Liechtenstein legal situation.

According to BGH judgment of 17.7.2009, 5 StR 394/08, whether a Compliance Officer is responsible for preventing legal violations at a company depends on their role and duties. This is because a Compliance Officer is responsible for ensuring that the company abides by the law and does not engage in illegal activity that could harm its reputation or lead to legal problems. In this role, Compliance Officers will regularly be classified as guarantors under criminal law.

Aside from contractual assignments, there is also a legal obligation to appoint a compliance officer under Art. 22 of the Liechtenstein Due Diligence Act (Internal Function of the Due Diligence Officer). Pursuant to Art. 22 in conjunction with Art. 34 of the Due Diligence Ordinance, Due Diligence Officers – who are responsible for ensuring the company follows the law – must comply with the law themselves. Compared to the relevant responsibilities of the Compliance Officer, this can justify a guarantor position in accordance with §2 LCC.

For this reason, when drawing up an employment contract, the scope of duties of the Compliance Officer should be defined as precisely as possible to be able to limit liability as a potential guarantor.

VI. EQUIVALENCE CORRECTIVE

However, an omission within the meaning of §2 LCC is only punishable if "the failure to avert success is equivalent to the realization of the crime by an act (equivalence corrective = equality clause[4]). This

[3] *Kienapfel/Höpfel*, Strafrecht AT[16], Z 29, 14.

[4] see *Kienapfel/Höpfel*, Strafrecht AT[16], Z29, 17.

is a kind of safety net, which in the overall view of all objective and subjective circumstances of the case is intended to prevent an excessive punishment for failing to act under certain circumstances.

In addition to the requirements of §2 LCC, the "general" requirements of criminal liability of the Compliance Officer must also be met for a Compliance Officer to be criminally liable. One such requirement is that the Compliance Officer must act with contingent intent (dolus eventualis) unless the law requires a different form of intent in individual cases. This is the case if the perpetrator considers the realization of a factual situation to be possible and resigns himself to it. With respect to failing to prevent a crime, or omission, intent exists if the Compliance Officer understands that:

i) he/she is a guarantor,

ii) there is compliance duty according to the situation,

iii) he/she would have to act and

iv) he/she nevertheless decides not to do anything.

If "this awareness and this decision to cease and desist are lacking, there is a lack of intent on omission.[5]

Finally, criminal liability presupposes that a Compliance Officer can also avert the punishable success. The possibilities available to prevent a crime depend on the competences provided for in the employment contract. A Compliance Officer will only be able to intervene an employee's misconduct if they have the authority if he has the appropriate authority to issue instructions. If such authority is lacking, an escalation to the management or responsible body of the company could be primarily considered. As a rule, this will already be sufficient to avert criminal liability for omission. As a preventive measure, reporting lines and a clear procedure for emergencies should therefore be defined in advance. Another conceivable measure would be the notification on the breach of law to a competent authority. In accordance with Article 17 of the Due Diligence Act, a Compliance Officer is obliged to do so as soon as there is a (albeit weak) suspicion of a predicate offence for money laundering or terrorist financing. A violation of this duty can ultimately result in contributory negligence or criminal sanctions due to ancillary criminal violations of reporting obligations.

VII. CONCLUSION: HOW CAN THE COMPLIANCE OFFICER PROTECT HIMSELF?

In principle, the Compliance Officer faces the same penalty as an employee who commits a crime for failing to prevent such crime. Therefore, if he deliberately looks the other way when the company acts in criminally relevant conduct, this can result in severe prison sentences and a possible professional ban (for lack of trustworthiness).

To be able to assess their criminal risks, Compliance Officers should pay particular attention to the terms of their employment contract and job description. It should clearly define the Compliance Officer´s obligations and competencies. In addition, care should be taken to ensure that the

[5] *Fuchs/Zerbes*, Strafrecht AT[11], Cap. 37, 67.

Compliance Officer also has appropriate instruction powers in those areas in order to ensure compliance with the law. Finally, it also makes sense to sign an appropriate D&O insurance contract to mitigate risks for personal liability.