DICO Guideline

G04 – Internal Investigations

Authors: Working group Internal Investigations

DICO
Deutsches Institut für Compliance

Status: November 2018

Disclaimer

DICO guidelines are aimed at compliance practitioners. They should facilitate an introduction into the topic and provide an overview. Therefore it is deliberately refrained from legal cases and derogations.

DICO guidelines provide the reader practical and implementable recommendations for selected compliance issues. With the publication of a guideline, a discussion is to be launched at the same time with a view to developing a standard that is recognized by compliance practitioners.

Please send your suggestions and contributions to info@dico-ev.de. We are looking forward to a lively discussion and thank you for your constructive support!

1. Introduction and Legal Framework

The detection of compliance violations and the appropriate reaction pose a particular challenge to all companies.
Often, there are already uncertainties concerning the scope of obligations to investigate and corresponding duties of directors suggested by circumstances that point at compliance violations within the company. Those signing responsible are confronted with considerable organizational challenges in terms of data protection and employment law throughout the preparation and implementation of investigative and disciplinary measures.

In the context of internal investigations, any violation of a duty may potentially trigger claims in damages vis-à-vis the company‘s management and even supervisory authorities. This is particularly true, where an internal investigation has been initiated while a follow-up on compliance violations is not sufficiently taken care of. Also the way in which an investigation is conducted, entails risks of prosecution and liability both for investigators and management bodies (e.g. data protection law).

Against this background board members and those responsible for conducting an internal investigation, should comprehensively update their knowledge about „their“ individual legal duties and with regard to potential consequences. Key legal obligations and outer boundaries are summarized below.

1.1. Obligation to clarify in case of suspicion

Today, it is widely accepted, that a company‘s management is under the legal duty to investigate indications of breaches of law and to delve into the facts. A company‘s management has no discretion as to „whether“ at all start investigating. Regarding the scope of an initiated investigation its discretion is largely restrained. On a more general note, the company‘s management should not be satisfied by incomprehensive or even incomplete investigations.

The company has to „get to the bottom of things“ and should carve out the facts. Yet, „how“ an investigation is conducted remains to the discretion of the management. Also, the decision as to „who“ carries out an investigation is at the management‘s disposal. It may direct others to execute an investigation – internally (e.g. to internal audit or to the compliance department) as well as externally (e.g.to lawyers and auditors).

Chapter 3 provides further guidance on the basic organization and scope of internal investigations.

The most important goal of an internal investigation is the legally compliant and, as far as possible, comprehensive substantiation of facts. To the extent that an investigation is conducted fairly, efficiently and professionally, the affected company may suffer more harm than good. An internal investigation is – contrary to public investigations – not subject to pre-defined procedural regulation.

It is rather in (large) parts constrained by data protection and employment law. However, companies that observe regular notifications, operate under a corresponding compliance risk profile or have suffered from previous compliance crises are recommended to define clear rules and procedures in a guideline for internal investigations („Compliance Investigation Guideline"). Chapters 2 and 4 below summarize recommendations to consider when drafting a Compliance Investigation Guideline.

Also, sanctions should be clearly defined and binding upon those applying them (in particular they should be objective, proportionate and transparent). To this end, the creation of a high-level „Group Compliance Committee" is recommendable. Its agenda – in addition to defining the internal organization – should comprise the development of basic rules for sanctioning.

1.2. Obligations under Data Protection Law

Data protection law is of paramount importance to internal investigations. Violations of data protection law triggers criminal liability for perpetrators, substantial fines, as well as a loss of profits and serious reputation damage resulting from negative media coverage.

Sec. 4 para. 1 of the Federal Data Protection Act (Bundesdatenschutzgesetz, **BDSG**) stipulates a preventive ban including a reservation for authorization for the collection, processing and use of personal data. Relevant to internal investigations is primarily sec. 32 para. 1 sentence 2 BDSG: it applies to all employees (including executive employees) and allows data collection, processing and use of employment data, wherever an offense has been committed in the context of a standing employment relationship. Furthermore, sec. 32 para 1 sentence 1 BDSG allows for the collection, processing and use of employees' personal data, to the extent necessary for establishing, executing or terminating an employment relationship. This rule may, if necessary, be used as a check-list of authorizations provided an action does not exclusively focus on detecting a criminal offense, but rather centers upon „merely" identifying violations of internal directives. For reasons of legal certainty it is, however, advisable to define the appropriate circumstances under which personal data may be processed directly in the articles of incorporation, which may constitute valid authorizations under the BDSG. In all cases, a full-blown test of proportionality (necessity, suitability and adequacy) shall be carried out. For those persons who are targeted by an internal investigation, who are, however, not „employed" within the meaning of sec. 32 BDSG, sec. 28 BDSG is applicable (i.e. members of a company organ and external persons whose data may possibly be collected, such as e-mail transmitters, etc.).

Pursuant to sec. 28 para. 1 no. 2 BDSG, the collection, processing and use of personal data is permitted if the company has conducted a test of legitimate interests, which revealed that the tested interests of the affected persons does not prevail. In these cases, it is equally important to carefully weigh the company's interest in conducting an investigation against applicable general rights to personality of those affected by it. When assessing the access to such e-mail accounts, that have previously been subject to authorized or tolerated (partial) private use, it is key whether or not the company is legally treated as a provider of telecommunications services in accordance with the Telecommunications Act (**TKG**). Respectively, providers of telecommunications services enjoy fewer rights and – in some cases – the necessary evaluation may even be inadmissible.

About DICO:

DICO – Deutsches Institut für Compliance e.V. was founded in November 2012 in Berlin at the urging of leading compliance practitioners and experts. As a nonprofit organization DICO has members from all industries in Germany, including wellknown DAX companies, auditing and law firms, and from the science industry.

DICO considers itself to be an independent interdisciplinary network for exchange between economy, science, politics, and administration and considers itself to be a central forum for the consistent and practical promotion and further development of compliance in Germany. DICO promotes compliance in Germany, defines minimum standards in this area, assists with proposed legislation, and simultaneously promotes practical compliance work in private and public companies, promotes training, and develops quality and procedural standards.

DICO – Deutsches Institut für Compliance

Chausseestraße 13

D-10115 Berlin

info@dico-ev.de

www.dico-ev.de