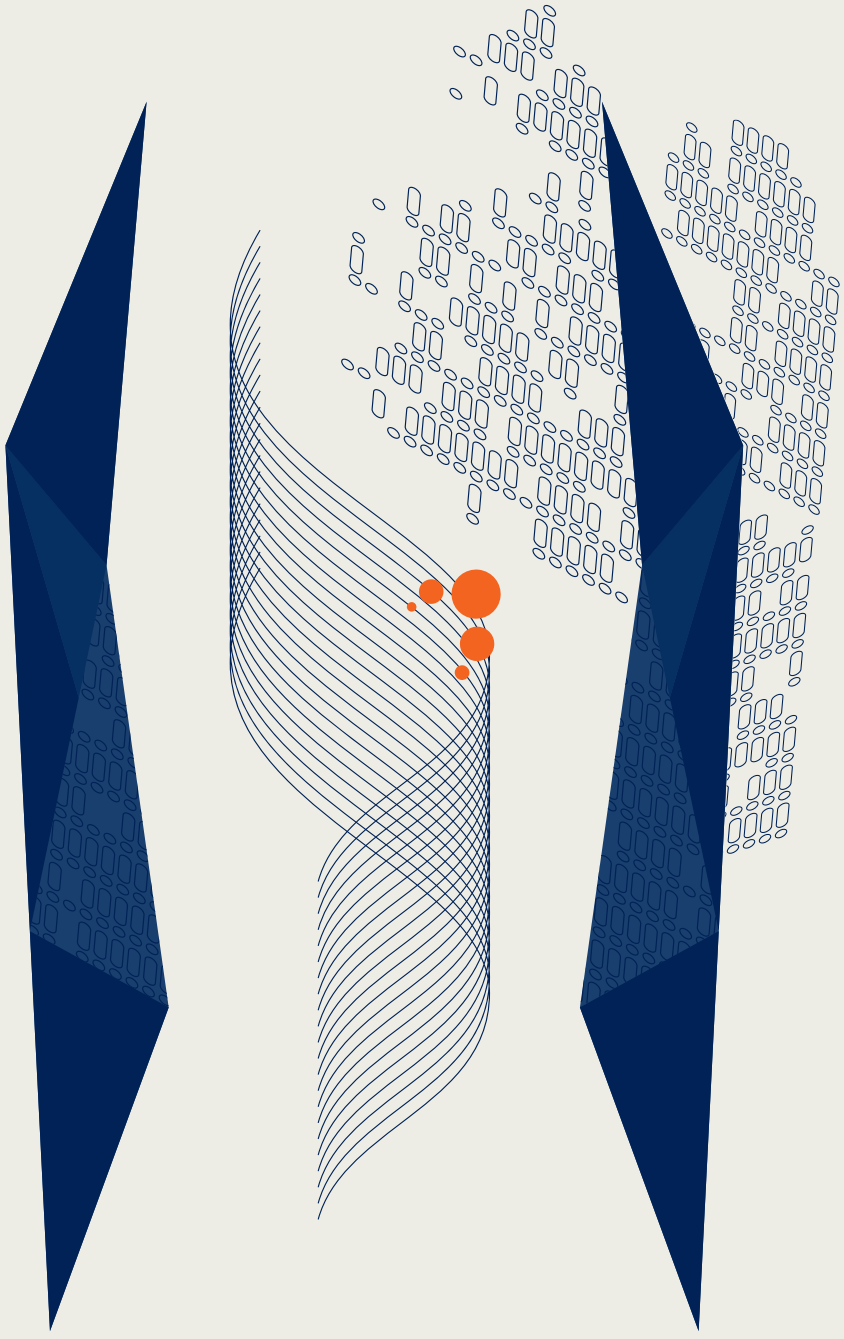
Digitalisation & Compliance

Executive Summary 2021



In cooperation with:

Technische Universität München

Noerr

Preface

Even though the Bundestag stopped the Federal Cabinet's draft bill on corporate sanctions law, which had already been passed in 2020, on the home stretch, the demands on entrepreneurs and compliance officers have noticeably increased in recent months.

Numerous new laws and regulations at federal and European level have come into force and mean additional work for those responsible.

Against this background, we are pleased to present our latest compliance study. We have once again conducted 300 interviews with managers of private-sector companies at the first and second decision-making levels and have summarised the results for you in a compact form - when reading it, you will certainly come across many interesting details.

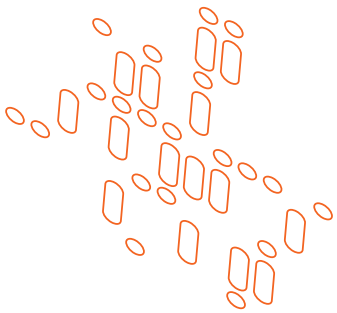
If you have any comments on the study or would like to provide ideas and impulses for future studies, please do not hesitate to contact us. We look forward to your feedback!

Professor Peter Bräutigam

Dr Julia Sophia Habbe

Professor Dirk Heckmann

Executive Summary



Advancing digitalisation is presenting companies with a range of organisational challenges. This also applies to compliance, as new technologies are creating new compliance risks. It is up to the management to identify these risks and allocate responsibility for tackling them correctly within the organisation.

Yet the companies surveyed by us often see themselves as inadequately positioned as far as their digital set-up is concerned, even though the need for action seems to be especially urgent in the area of compliance. This is even truer for smaller companies, which regard their level of digitalisation as being lower than that of large organisations. On top of this, many organisations lack dedicated positions for monitoring digital compliance risks and the technical expertise this calls for.

While the vast majority of companies in our survey have taken action and looked into the legal risks associated with digitalisation, many of them have nevertheless experienced such risks first-hand. The legal risks that can arise when using new technologies are especially underestimated. Often, there also appears to be a lack of risk awareness when it comes to using compliance tools.

The Covid-19 pandemic has given the use of digital work equipment an extra boost. The survey shows that many companies consider their use to be a concern from a compliance point of view. On the other hand, the coronavirus outbreak does not appear to have led to any compliance policies being relaxed.

Organising digital compliance is a management task

It is the management's job to identify digital compliance risks and to allocate responsibility for dealing with them correctly within the company. The responses to our survey suggest, however, that only a few companies see their management as being responsible for digital risks.

There is an urgent need for action. Management must take appropriate action to create and maintain the company's cyber security. Yet, according to the feedback received from the companies we approached, responsibility for digital infrastructure is often misjudged.

Many companies see themselves as having an inadequate digital set-up

Companies must have appropriate structures and processes in place to cope with the growing challenges of digitalisation. The majority of the managers surveyed see a need to catch up in this area and assess the digital readiness of their own company as being low to medium. Of the various corporate divisions, the compliance department performs the worst. Only one third sees a high to very high level of digital readiness.

As dedicated positions for digital compliance risks are often lacking, technical expertise is underrepresented

This self-assessment of limited digital readiness is also reflected in organisational terms. Many companies have not established dedicated positions for dealing with digital compliance risks, with around **70%** saying that they do not have such positions in place.

The professional background of compliance officers also shows a mixed picture. This may admittedly also be due to the fact that there is no reliable data available on the expertise required in this area. It is still the case that the majority of those entrusted with compliance tasks have a business management or law degree, while dedicated technical expertise appears underrepresented. Only slightly more than a quarter of compliance officers have a technical or IT background.

Around half of the companies surveyed have already experienced digital legal risks first-hand

Digital legal risks have increased in recent years. This finding is in line with the feedback received from the decision-makers questioned.

While the vast majority of companies surveyed have looked into the legal risks associated with digitalisation, with many of them identifying their risk exposure in SWOT analyses, around half of the study participants have already had first-hand experience of these legal risks, such as in the form of hacking attacks or data privacy breaches.

The legal risks posed by newer technologies are especially underestimated

It is notable that companies frequently underestimate the legal risks posed by newer technologies. In the area of cloud computing, artificial intelligence and big data analysis, about half of the companies surveyed rate the legal risks as being low. This perception, however, is at odds with the constantly growing regulatory requirements, such as those placed on data protection or IT security.

In its Schrems II ruling of 16 July 2020, the ECJ declared the "EU-US Privacy Shield" invalid and thus made legally compliant data transfers to the USA considerably more difficult. Yet, many cloud services are provided or hosted by US providers. Since supervisory authorities focus on ensuring that the transfer of personal data to third countries is data compliant, there is a risk of high fines and claims for damages by third parties affected by breaches.

Requirements under IT security law are also getting tougher. With the "German IT Security Act 2.0" passed on 23 April 2021, the Bundestag, as the lower house of German parliament, abandoned its sector-specific approach and extended the obligations under IT security law to include "companies of special public interest". In addition, from 1 May 2023 onwards "critical infrastructure operators" must use "attack detection systems". Violations can result in fines of up to €20 million.

Regulatory requirements are also increasing with respect to artificial intelligence and big data analysis. On 21 April 2021, the European Commission presented a draft "AI Regulation". The proposal follows a risk-based approach and in some cases places strict requirements on the technical structures and use of AI. If a company violates the prohibitions, the draft regulation provides for fines of up to €30 million or **6%** of its worldwide annual turnover.

While information and process tools are widespread, risk awareness remains low

According to the feedback received, information and process tools make up the majority of existing compliance tools. These include analysis and monitoring tools as well as e-learning platforms, for example. About a third of the companies use tools developed by them in-house.

However, the majority of respondents do not seem to be aware of the fact that the use of such tools can itself involve compliance risks. Only **32%** of the companies based abroad and **16%** of those based in Germany see risks in the use of compliance tools.

Use of digital tools is widespread despite compliance concerns

Even if companies tend to generally underestimate the legal risks brought by newer technologies, there is at least a certain awareness of compliance risks with regard to the digital work tools they use. For example, about a fifth of the decision-makers questioned state that video conferencing, SharePoint systems or collaboration tools involve high to very high compliance and data protection risks. Nevertheless, digital tools have become an integral part of today's working life. The Covid-19 pandemic has served to drive up their widespread use even further.

Hardly any relaxation of compliance policies during the pandemic

Few companies appear to have eased their compliance policies during the Covid-19 pandemic. Around two-thirds of respondents said that compliance policies in their industry had neither been suspended nor relaxed. This may come as a surprise, as many companies have had to find flexible solutions to counter the effects of Covid, for example through working from home. The number of unreported incidences of relaxed internal rules is therefore likely to be much higher.

Editor

Noerr Partnerschaftsgesellschaft mbB
Brienner Straße 28
80333 Munich
T +49 89 28628-0
www.noerr.com

TUM Center for Digital Public Services
Technical University Munich
Richard-Wagner-Straße 1
80333 Munich
T +49 89 907793-301
www.gov.tum.de/elaw
www.tum-cdps.de