

数字经济时代企业数据合规建设考察

——以合规计划有效建构为基点

肖 凤 刘 东*

内容摘要:数字经济时代,数据在企业的生产经营中的重要性日益凸显,已然成为企业经营中的一项重要生产要素。与此同时,部分平台企业违反数据法规案例引起了社会的广泛关注。在现有数据保护法律法规体系下,如何引导平台企业合规合法经营,让企业行稳致远,可以从建立健全企业数据合规的管理制度、数据的风险识别制度、数据风险的评估与处置制度、数据合规的运行与保障制度着手,加强企业合规计划的制度建设。从企业合规管理体系的有效设计、管理体系执行的有效、管理结果的有效三个层级对企业合规计划的有效性进行评估,来强化对企业合规计划的执行进行考察,以达到助力数字经济更好更优发展。

关键词:数据合规 合规计划 有效性 数字经济 企业合规 数据保护法规

信息技术的发展促进了经济向数字化转型,云计算、物联网、大数据分析与应用、区块链、人工智能等多项新兴技术逐渐与经济发展相融合,数据已成为企业经营中一项重要的生产要素。与此同时,涉及数据的违法犯罪行为也随之而来。数据合规经营是企业生存发展的必然要求,数据合规建设刻不容缓。

一、合规计划应遵循的法律规制

(一)数据、数据合规与合规计划

数据这个概念近些年引起公众的广泛关注,主要是因为移动互联网、大数据、云计算、人工智能等科技迅猛发展,导致数据的产生和处理呈现爆发式增长,而基于大数据的一系列应用则深刻地影响着我们每个人的生活。^[1]同时,数据是继土地、劳动力、管理、技术、资本等之后的生产要素新形态,是优化生产资源高效配置、创造数字经济生产力、探索构建数字经济新型生产关系的新基因,更是促进数字经济和实体经济深度融合、推动经济高质量发展和构筑国际竞争新优势的新动能。从本质上来看,数据是信息的表现形式和载体。而法律意义上的数据,则是指任何以电子或者其他方式对信息的记

*肖凤,上海市杨浦区人民检察院检察官助理;刘东,上海市杨浦区人民检察院检察官助理。

肖凤负责总体框架与撰写,刘东负责收集资料与撰写。

[1]参见王倩、顾雪莹:《GDPR下涉欧企业的员工个人数据合规管理》,《德国研究》2021年第2期。

录。数据与信息的关系可以概括为数据是信息的载体、信息是数据的内容。^[2]根据数据内容的不同,可以将数据划分为个人信息类数据、企业信息类数据、公共信息类数据、混合信息类数据以及其他信息类数据。

1. 数据合规

数据合规,是指企业及其员工的经营管理行为符合个人信息保护、网络安全、数据安全等法律法规的要求。数据合规属于企业专项合规的一个重要类型,重点研究企业主体如何在经营活动中确保各类数据的全生命周期处理活动符合合规要求。数据合规对于企业、个人、社会均具有重要意义。^[3]一是帮助企业防范法律风险,或者在发生法律风险时减轻、免除企业责任,从而实现企业的可持续发展。^[4]二是避免个人信息等遭受不合理甚至违法泄露、滥用。数据泄漏和滥用严重威胁个人权益、财产安全甚至生命健康。避免企业滥用用户信息,促进企业依法合理使用个人数据,对于保护个人隐私和保障消费者权益具有重要意义。^[5]三是规范数字经济发展轨道,推动数字经济蓬勃发展。强化企业数据安全管理,维护好用户数据权益及隐私权,有助于提高数据共享意愿,最终推动数字经济走向繁荣。

2. 数据合规计划

在当下的语境里,合规计划是指一套完善的规章制度,通过实施并实现该制度可以帮助企业避免在一定领域内违法的风险。从企业自身视角看,合规计划是一种公司治理方式,企业要想获得好的发展,须在发展过程中采取一种管理模式,尽量避免内部发生违法犯罪行为及其带来的危害。

因此,数据合规计划的内涵可以总结为企业为预防涉及数据犯罪、发现数据犯罪而主动制定、实施的自我管理和约束机制,这种机制在员工或者企业涉罪时可以作为抗辩理由来减轻或者避免刑事责任。^[6]其本质上是一种广泛的预防措施,可以预测、检查并遏制任何潜在的犯罪活动。^[7]2021年可以称之为数据合规计划的元年。在立法层面,数据安全法、个人信息保护法陆续颁布实施,与网络安全法共同构成了我国数据法规的基本体系。在执法层面,滴滴、阿里等违反数据法规案例等均引起了社会的广泛关注,以个人信息滥用为主要诟病的数据风险事件屡禁不止也引发了舆论对于数据合规的热烈讨论。^[8]在监管层面,推动数字经济健康发展,要坚持促进发展和监管规范两手抓、两手都要硬,在发展中规范、在规范中发展。数据合规计划对于企业经营管理越来越重要,数据产业也必须围绕合规的框架发展完善。

(二)我国对数据的法律法规保护体系概述

我国对数据的保护,可以追溯到2012年全国人大常委会已经发布了《关于加强网络信息保护的決定》。2013年工信部发布了《电信和互联网个人信息保护规定》。在之后的4年中,对于数据和个人信息的规定寥寥。直至2017年的网络安全法。至2021年8月20日个人信息保护法,2021年6月10日数据安全法出台,自此我国以网络安全法、个人信息保护法为三大支柱的数据合规法律制度体系已基本建立。其中网络安全法是我国第一部全面规范网络空间安全管理方面问题的基础性法律,规范在我国境内建设、运营、维护和使用网络,以及网络安全的监督管理活动。我国网络安全法的基本原则包括网络空间主权原则、网络安全与发展并重原则、责权利相统一原则和共同治理原则等四项基本原则。^[9]数据

[2]参见张勇:《数据安全分类分级的刑法保护》,《法治研究》2021年第3期。

[3]参见蒋安杰:《数据合规高端论坛在京举行》,《法治日报》2021年9月29日,第009版。

[4]参见刘霜:《意大利企业合规制度的全面解读及其启示》,《法治与社会发展》2022年第1期。

[5]参见于冲:《数据安全犯罪的迭代异化与刑法规制路径——以刑事合规计划的引入为视角》,《西北大学学报(哲学社会科学版)》2020年第5期。

[6]参见李勇:《“合规计划”中须有刑法担当》,载https://www.spp.gov.cn/spp/llyj/201805/t20180524_379571.shtml,2023年2月2日。

[7]参见[美]菲利普·韦勒:《有效的合规计划与企业刑事诉讼》,万方译,《财经法学》2018年第3期。

[8]参见唐林焱:《数据合规科技的风险规制及法理构建》,《东方法学》2022年第1期。

[9]参见谢永江:《论网络安全法的基本原则》,《暨南学报(哲学社会科学版)》2018年6月第6期。

安全法是一部专门规范在我国境内开展数据处理活动及其安全监管的法律。个人信息保护法是我国第一部专门规范个人信息保护的专门法律。

除前述网络安全法、数据安全法、个人信息保护法加强对数据的保护外,数据保护还涉及民法典、密码法、电子商务法等其他法律;《互联网信息服务管理办法》等行政法规;《上海市数据条例》《深圳经济特区数据条例》等地方性法规;以及《大数据安全管理指南》《金融数据安全-数据安全分级指南》《个人信息安全规范》《个人信息安全影响评估指南》《网络安全等级保护基本要求》《网络安全等级保护测评要求》《网络安全标准实践指南-移动互联网应用程序(App)使用软件开发工具包(SDK)安全指引》等国家及行业标准中亦有对数据保护的相关规定和要求。

与此同时,域外也在逐渐加强对数据安全和个人数据信息的保护,如,2018年5月,欧盟出台了《通用数据保护条例》,旨在创建欧盟统一的数据与隐私保护法;2018年6月,美国紧随其后,出台了《加利福尼亚消费者隐私法案》,该法案被认为是美国史上对消费者隐私保护最为全面的法律。^[10]综上可知,大多数国家都非常重视对数据的法律保护,企业在境外国家或地区的数据安全风险日益增加,各个国家或地区争相制定数据治理规则,对数据的产生、收集、存储、流动等活动进行规范。因此,对于企业数据跨境流动时,还要遵循所在国家或地区数据保护的法律法规。

二、数据合规的制度建设

在数字经济时代,传统数据安全问题 and 新型数据安全风险相互叠加,数据合规是现代企业治理体系在大数据时代诞生的新内容,强调企业以自身的努力积极防范数据刑事安全风险,把与数据相关的犯罪消除在萌芽状态。而数据合规制度建设是指相关企业针对数据风险,制定数据合规整改计划,完善企业治理结构,健全内部规章制度,形成有效合规管理体系的活动。从制度上建设数据合规,可以实现企业内部治理的裂变,促进企业合法守规经营,让数据成为企业真正的优质资产,最大限度提升企业抗风险的能力。

(一)数据合规的管理制度

1.合规责任人与数据合规管理部门

企业董事会应当向数据合规管理部门负责人提供足够的授权、人力、财力等资源支持数据合规管理体系的运行。一般由董事会直接设立企业合规部门、任命首席合规官,下设数据合规管理部门等各类专业合规部门。董事会应当承担以下职责:(1)分配足够和适当的资源来建立、发展、实施、评估、维护和改进数据合规管理体系;(2)举报机制;(3)确保战略和运营目标与履行数据合规义务之间的一致性;(4)建立责任追究机制;(5)确保将数据合规落实情况 and 效果纳入企业内部人员绩效考核体系。鼓励各类企业设置专门的数据合规管理部门,或者将数据合规管理职能融入现有的企业合规管理体系。

2.数据合规管理部门的职责

数据合规管理部门应履行以下职责:(1)制定合规计划总的方针政策,做好风险防范指引;(2)结合企业自身的经营范围、行业特征、监管政策、风险识别等因素制定并不断完善数据合规计划,并推动其有效实施。数据合规计划应当提高企业面对负责环境的适应能力,帮助企业提高抵御风险能力。(3)审核评估企业的经营管理和业务行为,确保企业与客户、供应商、代理商、经销商、关联企业、分支机构等业务活动,以及处理个人信息等活动符合数据法规的要求,并制定数据风险应对措施;(4)组织或协助管理部门、业务部门等开展数据合规教育培训,并向管理层和各部门员工提供数据合规咨询;(5)建立数据合规举报记录台账,对数据合规举报制定调查方案并开展调查;(6)推动将数据合规责任纳入企业岗位职责和员工绩效考核评价体系,培养数据合规文化;(7)持续关注相关国家(地区)数据法律

[10]参见刘鑫:《数据合规——强数据监管时代下的必然选择》,载《国浩律师事务所》微信公众号,2022年4月3日。

规制情况,为企业经营提供建议。

3.数据合规管理协调

数据合规管理部门应加强与业务部门的分工协作。应积极与数据监管部门建立沟通渠道,了解数据监管部门期望的数据合规体系,并制定符合其要求的数据合规制度;业务部门应当根据企业的合规制度和要求,制定具体业务中的合规计划,并查找、摸排风险点,进行负面评估以及堵塞漏洞;业务部门在评估过程中,发现的存在重大数据风险的事项,要及时向合规管理部门报告,管理部门可以向数据监管部门咨询。此外,企业要积极配合数据执法监管部门的执法、调查。

(二)数据的风险识别制度

建立数据风险识别制度是企业数据合规的应有之义。常见的数据风险包括数据全生命周期各阶段中可能存在的未授权访问、数据滥用、数据泄漏等风险,以及侵犯个人信息、非法获取计算机信息系统数据、传播违法信息、侵犯知识产权、非法跨境提供数据等刑事犯罪风险,企业应根据识别出的风险评估相关经营管理和业务行为是否合规。^[11]与此同时,企业要立足自身实践,建立符合自身的合规计划,并通过完善内部自上而下的合规责任链条和自上而下的信息流与自下而上的信息流,以及外部“外脑”咨询的助力,加强对数据监管最新情况的跟进,以便准确识别数据风险。

1.禁止从事的数据活动

企业及其员工开展数据处理活动应当遵守法律、行政法规,尊重社会公德和伦理,不得从事以下活动:(1)危害国家安全、荣誉和利益,泄露国家秘密和工作秘密;(2)侵害他人合法权益的行为;(3)通过不合法方式获取数据;(4)任何个人和组织知道或者应当知道他人从事前款活动的,不得为其提供技术支持、工具、程序和广告推广、支付结算等服务。

2.常见的数据风险

网络安全审查。数据处理者处理个人信息等数据应当符合数据法规的规定,开展影响或者可能影响国家安全的数据处理活动,应当根据国家有关规定,申报网络安全审查。

自动化工具。数据处理者在采用网络爬虫等自动化工具访问、收集数据时,应当评估对网络服务的性能、功能带来的影响,不得干扰网络服务的正常功能。自动化工具访问、收集数据违反法律、行政法规或者行业自律公约、影响网络服务正常功能,或者侵犯他人知识产权等合法权益的,数据处理者应当停止访问、收集数据行为并采取相应补救措施。

软件开发工具包。企业在应用程序开发和运营过程中使用第三方软件开发工具包时,应当通过合同等形式明确第三方的数据安全责任义务,并督促第三方采取必要的数据安全保护措施,加强数据合规管理。企业可以使用经相关部门审核合规的开源软件开发工具包进行程序开发活动,不得使用风险不可控的开源软件开发工具包等工具。

3.对外提供个人信息

数据处理者向第三方提供个人信息,或者共享、交易、委托处理重要数据的,应当遵守以下规则:(1)向个人告知提供个人信息的目的、类型、方式、范围、存储期限、存储地点,并取得个人单独同意,符合法律、行政法规规定的不需要取得个人同意的情形或者经过匿名化处理的除外;(2)明确数据处理权利义务;(3)留存个人同意记录及提供个人信息的日志记录,共享、交易、委托处理重要数据的审批记录、日志记录至少五年。数据处理者为订立、履行个人作为一方当事人的合同所必须向第三方提供个人信息的,在采取适当的数据保护措施后无须取得个人单独同意。(4)数据接收方应当履行约定的义务,不得超出约定的目的、范围、处理方式处理个人信息和重要数据,且不得从事数据法规禁止的行为。

数据处理者因业务等需要,确需向中华人民共和国境外提供数据的,应当符合法律法规关于跨境提供数据的规定,事先开展数据出境风险自评估,并应当遵守相关法律法规的规定。

[11]参见裴炜:《刑事数字合规困境:类型化及成因探析》,《东方法学》2022年第2期。

(三)数据风险的评估与处置制度

1.数据风险评估

企业在识别数据风险内容的基础上,可根据自身经营规模、组织体系、业务内容以及市场环境,分析和评估数据风险的来源、发生的可能性、后果的严重性等,并对数据风险进行分级。数据合规部门负责人应当根据风险评估结果对不同职级、不同工作范围的管理层与员工进行风险提示,降低管理层和员工的违法犯罪风险。

2.数据风险处置机制

企业应建立健全数据安全事件应急预案与风险处置机制,对识别和评估的各类数据风险设置恰当的控制和应对措施来降低风险,必要时停止相关风险行为。

风险事件报告义务。发生个人信息等数据泄露、篡改、丢失等事件的,数据处理者应当立即采取补救措施,并通知所在地区的数据监管部门。涉嫌违法犯罪的,应及时向移交司法部门。

立即停止违法行为。经评估发现可能已经存在数据违法行为应立即停止,在留存相关证据的同时立即开展补救措施。如果发现监管部门已立案并启动调查程序的,应当主动配合并与执法机构合作。

反应、制裁和改进。反应,是指发生违法犯罪行为之后,企业应该采取怎样的态度和措施来规制违法犯罪行为。如发现违法犯罪行为以后,企业要进行内部调查。内部调查所获得的这些证据,应及时向监管部门或者司法部门披露,因为合规制度本身一个很重要的价值就在于助力司法效率的提升。制裁,是指发生违法犯罪行为之后企业采取什么方式进行惩处,对违规行为和合规行为的处理措施要有显著的区分。改进,是指针对违规行为发生后,企业要采取相应的措施对企业的合规机制进行查漏补缺。

投诉举报渠道。企业应当建立投诉举报渠道,并及时受理。企业应当公布接受投诉、举报的联系方式、责任人信息,每年公开披露受理和收到的数据安全投诉数量、投诉处理情况、平均处理时间情况,接受社会监督。

(四)数据合规的运行与保障制度

1.合规咨询与发现机制

企业可建立数据合规咨询机制,管理层和各部门员工在工作中可以向数据合规管理部门咨询数据合规问题。数据合规管理部门应当不断学习、提升合规管理水平,也可以同外部机构开展数据合规咨询合作。发现机制是数据合规管理部门通过日常监测和定期评估发现数据不合规行为的机制,可以通过设置日常的流程监控、内部审核、重点核查以及定期评估等方式发现企业及员工的违规行为,并及时按照合规计划采取相应的处置措施。数据合规管理部门应定期向合规负责人汇报数据合规管理情况。当发生可能给企业带来重大数据合规风险的违规行为时,应当及时向合规负责人汇报,并提出相应的解决方案。

2.举报与考核奖励机制

建立举报机制。举报机制是员工根据合规计划举报企业内部违规行为的机制,应当允许员工实名或者匿名通过内部举报系统举报数据违规行为,并严格保护实名举报者和匿名举报者不受打击和报复,尤其是保护匿名举报者的个人信息安全,适当条件下可以予以一定形式的奖励。企业可以将数据安全与合规遵从纳入企业内部绩效考核管理当中,对于严格遵守数据合规的管理层和员工,制定适当的激励措施,对发生数据安全或违规事件的人员进行惩罚,以确保企业数据合规管理制度和体系的权威性和有效性,保障企业数据合规管理体系的可持续性和生命力。对于不严格执行甚至违反合规计划的管理层和员工,采取适当的纪律措施进行惩戒,并根据违规程度采取不同的风险处置措施。

3.培训、承诺、信息化建设机制与合规文化

数据合规管理部门应当建立培训机制,定期为管理层、员工培训数据合规,使其充分了解数据法规、数据合规计划、岗位角色与职责等。鼓励企业管理层和其他员工作出并履行明确、公开的数据合规

承诺,内容主要是知悉、愿意遵守数据合规计划,愿意承担违反数据合规承诺的后果。企业可通过信息化建设,运用大数据分析等工具,查找分析企业业务运行过程当中,可能会涉及的风险点,并进行数据合规的实时监控和风险评估。鼓励企业将数据合规文化作为企业文化建设的重要内容,践行合规经营的价值观,不断增强员工的数据合规意识。

三、合规计划的有效性评估

数据合规计划评估指的是第三方监督评估组织对涉案企业数据合规整改计划和相关合规管理体系有效性进行了解、评价、监督和考察的活动。包括:对风险的识别、控制;对违规违法行为的查处;合规管理人员的配置;合规管理制度机制建立以及人力物力的充分保障;监测、举报、调查、处理机制及合规绩效评价机制的正常运行;持续整改机制和合规文化已经形成。结合数据行业的特点与美国企业合规计划评估方法,数据合规计划评估可以从设计的有效性、执行的有效性与效果的有效性三个方面来开展,具体包括责任人和管理架构、规范和制度、合规承诺、合规文化等十二个维度。以此实现对企业数据合规建设情况的评估,促进第三方监督评估有规可循。

(一)企业合规管理体系的设计

1.责任人和管理架构

企业的最高管理者(董事会主席、总裁等最终决策者)是数据合规的第一责任人,应当分配足够和适当的资源来建立、发展、实施、评估、维护和改进数据合规管理体系。一般而言,从专业性角度,条件允许的企业要有企业合规官、合规部门的设置,在专业部门的设置下要配备专业人员进行合规治理和运作。因此,由董事会直接设立企业合规部门、任命首席合规官,下设数据合规管理部门等各类专业合规部门。尚不具备条件的企业,可以有一定层级的高管兼任。企业可以在与数据处理有关的内设部门设立相应的专职或兼职的管理岗位,定期收集、整理与反馈相关信息至合规部门。

2.规范和制度

企业应当根据我国法律法规,参考国际国内技术标准,结合企业自身的经营范围、行业特征、监管政策、风险识别等因素制定并不断完善数据合规计划。同时,企业可以制定员工准则、操作规范、业务守则等具体规范,明确员工应当遵守的数据合规义务。企业应采取一定的措施确保数据合规计划等规范具备设计的科学性、更新的及时性,以及实施的全面性、深入性。

3.风险识别、评估和处置

企业应当全面、系统、持续地收集内部和外部相关信息,综合考虑行业属性和企业自身特点,准确识别企业经营活动及其业务流程中的数据风险。常见的数据风险包括收集、传输、存储、加工、使用、提供、公开、删除等数据全生命周期各阶段中可能存在的未授权访问、数据滥用、数据泄漏等风险,以及侵犯个人信息、非法获取计算机信息系统数据、传播违法信息、侵犯知识产权、非法跨境提供数据等刑事犯罪风险。

企业在识别数据风险内容的基础上,可根据自身经营规模、组织体系、业务内容以及市场环境,分析和评估数据风险的来源、发生的可能性、后果的严重性等,并对数据风险进行分级。然后根据风险评估结果对不同职级、不同工作范围的管理层与员工进行风险提示,降低管理层和员工的违法犯罪风险。

企业应当定期测试数据风险识别与评估的有效性,重点关注企业特定业务范围内最有可能发生的数据安全事件,并根据识别与评估结果及时修订数据合规计划。

企业应建立数据安全事件应急预案与风险处置机制,对识别和评估的各类数据风险设置恰当的控制和应对措施来降低风险,必要时停止相关风险行为。

发生个人信息等数据泄露、篡改、丢失等事件的,企业应当立即采取补救措施,并通知所在地区的数据监管部门。数据泄露、篡改、丢失等涉嫌刑事犯罪的,在报案的同时将相关线索及时移送司法机关。

4.培训和沟通

企业应当建立培训机制,定期为管理层、员工培训数据合规,使其充分了解数据法规、数据合规计划、岗位角色与职责等,确保员工理解、遵循数据合规目标和要求。应建立数据安全沟通制度,确保处理数据的员工与企业网络安全部门、数据合规管理部门等中高层管理层的定期沟通和反馈,并和数据监管机构保持良好沟通。

5.举报和调查

应当允许员工、客户和第三方实名或者匿名通过邮箱、电话等途径举报数据违规行为,并严格保护实名举报者和匿名举报者不受打击和报复,尤其是保护匿名举报者的个人信息安全。员工、合作伙伴或第三方被举报或者监测到可能存在违规、违法或犯罪时,企业应及时针对举报信息、违规线索展开彻底的内部调查,由合规管理部门或其他受理举报的监管部门制定调查方案,明确组织调查的人员和范围,调查响应方式等,并规定不同调查结果下的处置方式。

6.第三方关系风险评判

企业应当关注关联企业、供应商、经销商、代理商、合作企业等第三方的合规建设情况,尤其是与第三方发生关系时可能产生的数据风险。企业向第三方提供个人信息,或者共享、交易、委托处理重要数据的,应当要求数据接收方履行约定的义务,不得超出约定的目的、范围、处理方式处理个人信息和重要数据,且不得从事数据法规禁止的行为。

(二)管理体系执行的有效

1.合规承诺

企业管理层和其他员工应作出明确、公开的数据合规承诺,内容主要是知悉、愿意遵守数据合规计划,愿意承担违反数据合规承诺的后果。企业各级管理层应当带头履行合规承诺,在日常经营管理中阐明、引导、鼓励员工遵守数据合规要求和具体准则,并进行合理监督。

2.授权和资源

企业应当向数据合规管理部门提供足够的授权、人力、财力来支持数据合规管理体系的运行。企业可以通过数据合规管理信息化建设和大数据分析等工具,加强对经营管理行为中的数据合规的实时监控和风险分析。

3.激励和纪律

企业应当建立数据合规考核机制,数据合规考核结果作为企业绩效考核的重要依据,与员工的薪酬待遇等挂钩。

对于不严格执行甚至违反合规计划的管理层和员工,企业应采取适当的纪律措施进行惩戒,并根据违规程度采取不同的风险处置措施。

(三)管理结果的有效

1.合规文化

企业形成数据合规价值观,能够按照合法、正当、必要和诚信原则开展数据处理活动。企业能够对潜在的和客观存在的数据风险进行系统全面的识别和分类,分析风险产生的原因和过程,分析风险的源头,制定应对策略。企业管理层和员工能够学习并了解有关法律法规和数据安全管理标准,熟悉并遵守数据处理的基本流程和注意事项。

2.持续改进

企业能够根据法律、政策的调整及时修订数据合规计划等具体规范,不断完善数据风险识别、评估与处置体系。企业能够通过不定期的主动检测等方式,发现合规体系的不足并加以改进,同时根据

企业自身发展情况和数据处理的规范要求,进行差异化分析,确定部分特定风险领域是否得到充分重视。企业至少每年开展一次数据合规计划有效性的全面评估,根据评估效果持续改进数据合规计划。

3. 违规事件

发生违规事件并不意味着企业合规管理体系是无效的,但是从结果的意义上来讲,其一定是能够降低发生率的。因此,在发生违规事件后,要进行及时的自查,只有企业合规管理体系能够在合理时间内发现违规行为,并按照计划及时补救和报告,才可以认为该企业合规管理体系是有效的。

企业能够对违规事件开展独立客观的调查,分析违规原因,采取补救措施和追究责任,例如对违规事件予以内部通报,做好警示教育,从而降低相同或类似问题再次发生的风险。违规事件若涉及违法犯罪,企业应及时移交行政监管部门或司法机关处理,保持与有关国家机关的有效沟通,并提供必要的工作支持。

结 语

合规计划的制定和实施涉及了企业管理的多个方面,包括治理结构、规章制度、人员管理、报告机制等等,是企业的自我革新。同时,有效的合规计划离不开制定者科学的风险分析与评估,更离不开执行者坚定有力的执行。合规计划,如果只是一堆无法嵌入企业发展中的规章制度,最终将被束之高阁,成为一纸空文。因此,合规计划的有效落地和平稳推进,是数据合规的落脚点和关键点。企业不仅应建立行之有效的合规计划,还应将合规计划落到实处,只有如此才能助力企业的更好发展,才能让法治更好助力社会治理水平和治理能力的提升,才能促进数字中国的更好建设。