DOI:10.13395/j.cnki.issn.1009-0061.2024.07.006

数字经济时代企业数据合规难点与应对

——以 App 个人信息合规为视角

龚照绮,官中奇

(西南政法大学,重庆 401120)

摘　要:近年来,以数据资源为要素的数字经济发展迅速,同时给自然人的个人信息带来了极大的威胁。尽管中国通过立法明确了企业需履行保护个人信息的法定义务,但涉及个人信息的侵权行为、犯罪行为时有发生。本文旨在通过对企业在数字经济时代数据合规的难点分析,并从数据层、隐私政策层、权限层、制度组织层四个方面入手,找到应对措施,确保在满足法律监管要求和实现经营目标的情况下履行 App 个人信息保护的义务,最终实现 App 个人信息的合规处理。

关键词:数字经济;企业合规;个人信息保护

中图分类号:F713.36　　**文献标志码**:A

一、问题的提出

《"十四五"数字经济发展规划》明确提出健全完善数字经济治理体系和着力强化数字经济安全体系,推进数字经济法治化建设。在数字经济时代 App 得到广泛应用, 而在数字经济法治化建设过程中,App 的合法合规,是重要组成部分。在 App 快速发展过程中,随着《网络安全法》《数据保护法》《个人信息保护法》的实施,App 个人信息合规将是每家 App 运营公司的必答题。

目前《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律共同构建了 App 个人信息合规治理的基本法律框架。同时,网信办、市场监督管理局、工信部等部门针对 App 的监管逐渐加强,提出了明确的规定。法律赋予了公民充分的权利并强调个人信息处理者的合规义务,因此 App 运营企业需要主动适应数字经济法治化建设的法律要求。

二、企业开展 App 个人信息合规的必要性

(一)满足法律监管要求

企业作为 App 的运营方、作为个人信息的处理者,通过 App 为用户提供产品和服务的同时收集大量用户个人的信息。一方面,企业需要依据法律法规开展个人信息合规工作;另一方面,企业开展员工激励、市场活动、供应商竞标等经营活动时,需要大量的个人信息作为决策参考。因此,企业开展个人信息合规既是满足法律监管的要求,也是企业实现经营目标的需要。2021 年 11 月 1 日《个人信息保护法》正式实施,奠定了中国个人信息保护的法律基础,填补了针对个人信息保护的立法空白。企业在运营 App 为用户提供产品和服务时,面对众多法律法规及规范性文件的监管要求,企业需从中厘清法定义务,将义务转化为企业制度和实施流程。

(二)实现企业经营目标

企业作为 App 开发运营者,是 App 开发和运营活动的主体。App 作为企业重要的产品,承载企业众多市场服务功能,不仅是企业重要的生产经营的载体,也是企业与用户沟通交流的工具。近几年来,大数据、人工智能等技术在 App 的运用,提升了企业的生产能力以及用户的服务水平,促进企业实现经营目标。从 App 的功能设置层面,往往在用户首次使用 App 时, 便会被收集用户的注册登录、Cookie 等个人信息。在用户使用阶段,将会收集用户的互动数据、地址信息、用户偏好等个人信息。最后伴随着用户不再使用 App 服务而注销,至此 App 收集个

收改日期:2024-05-14

作者简介:龚照绮,西南政法大学马克思主义学院硕士研究生,西南政法大学党内法规研究中心研究员;官中奇,首都经济贸易大学工商管理学院硕士研究生,信息化百人会兼职研究员。

人信息将会结束。在用户从注册到注销的整个阶段,企业在运营 App 时为满足用户需求,提供产品和服务,都会收集用户的个人信息,企业收集的个人信息经过清洗、脱敏、标记、计算等的处理后,作用于企业的经营、市场等活动便会产生经济价值。例如 Shapiro 和 Aneja(2019)估计,2018 年,主要互联网搜索引擎、社交媒体平台、信用卡公司和医疗数据业务收集的美国人个人数据所实现的货币化相关收入超过 780 亿美元。数据为企业在数字经济时代的发展提供了内生动力,助力实现企业的经营目标。

三、企业开展 App 个人信息合规难点分析

无论是从法律监管还是企业实现经营目标,企业都必须开展个人信息合规工作,但实际情况却并非如此。从企业内部来看,企业往往是被动合规,应付监管,合规动力不足,难以形成较为完善的合规体系,致使企业的经营存在个人信息合规风险。同时,企业开展个人信息合规还面临很多认识上的误区,例如企业管理层认为个人信息合规是安全问题、技术问题,购买安全产品即可解决问题或认为合规工作只是安全部门或法务部门的工作,与其他部门无关。此外,企业还面临人才缺失,从国内立法来看个人信息保护不仅是法律问题,也是安全、管理、技术研发等问题。因此往往需要复合型的合规人才,以法律为基础,厘清法律的合规基线,同时构建企业管理制度、安全措施、合规嵌入开发流程等举措才能使得企业的个人信息合规落到实处。

从企业外部来看,中国个人信息相关保护制度,早在民法、消费者权益保护法中有所规定。但《个人信息保护法》实施的时间较短,以至于配套的司法解释、司法案例、指导性规范性文件等比较欠缺,致使个人信息保护的法律体系尚不健全。同时,还存在部分国标内容与法律相违背的情形。中央及各地主管部门竞相开展 App 治理,中央各部门之间、中央和地方主管部门之间,在认定 App 违法违规收集使用信息时,基于监管资源、监管风格的差异,众多监管主体之间难以做到统一标准。在事实上还可能会导致甚至加剧“多头”治理,导致个人信息保护行业生态发展无所适从的尴尬局面。

四、企业开展 App 个人信息合规解决方案

如何根据法律法规的要求,利用规范性文件、国际标准、国家标准、最佳实践以及司法案例,针对 App 所涉及的个人信息制定企业合规计划,实施合规方案是企业需要思考的问题。因此,笔者将从数据层、隐私政策层、权限层、制度层等角度分析企业所需要采取的合规动作,希冀为企业开展个人信息合规提供决策参考。同时,App 个人信息合规是一个动态的过程,未来依然需要依据新的政策动向和法律法规予以适当调整。

(一)数据层

1.数据盘点。在 App 上线前,企业首先需要开展数据盘点工作,通过开展数据盘点,厘清、清洗、整理和完善企业相关业务活动所产生的数据库、文件文档、字段代码等数据,同时将数据进行标签化和构建目录,提升数据可读性和可用性。企业可以从业务出发,分析 App 存在的业务目的、业务范围等(图 1)。

图 1 数据收集流程

数据盘点主要有以下步骤:

(1)数据收集。根据 App 的业务或功能,划分数据范围制定《数据清册表》,从而规范统一数据基本信息,便于构建数据标签化和构建目录。参与的组织可由企业数据合规部门、行政部门、技术部门以及外部律师或技术团队构成,数据收集时应当遵循合法、全面、真实、动态的原则。依据数据盘点收集表,将收集工具和具体的业务部门进行链接,并指定 1–3 名人员进行配合,主要采集对象包括系统数据库、文件文档、字段代码等。

(2)数据识别。根据 App 功能或服务实现所需要的个人信息实际情况,进行数据识别。同时在 App 测试上线前的阶段,可以通过技术手段针对个人信息、Cookie 信息进行识别并进行日志记录,对于收集的不完整的个人信息进行过滤。同时通过人工识别将其中涉及法律法规和指南标准规定的数据内容进行有效识别,从而判断是否可以收集,是否满足最小必要性等法律原则。

(3)数据清册。根据识别结果统一编辑数据清册,并对于个人信息所涉及的敏感个人信息进行单

独分类。同时,还需要在数据清册中增加有关该功能或服务收集个人信息的使用目的、数据流转情况、数据处理时的安全措施、数据跨境、数据共享等内容。以便于通过数据清册,整体了解数据的合规性和安全性以及收集该数据的业务的风险高低。

2.数据分类分级。在数据盘点的基础上,企业应建立数据分类分级管理制度,数据分类分级的对象通常是数据项、数据集,针对不同类别、级别的数据进行不同的权限设置,从而达到针对性的管理与保护。根据《网络安全法》《数据安全法》的相关规定,明确了网络运营者开展数据分类分级保护制度的责任。在分类层面,根据现行规范性文件以及国家标准如 GB/T4754–2017《国民经济行业分类》《中国移动大数据安全管控分类分级实施指南》等。也可从企业业务形态进行分类,可以分为生产数据、经营数据、员工数据、用户数据、市场数据、产品数据、位置数据、安全数据、运维数据等。在分级层面,可充分参考国家标准、实践指南等文件,将分级细化,在分级中要考虑影响对象、影响程度两个要素。我们还需认识到,数据的分类分级,既是数据合理开发利用重要的第一步,也是满足数据的安全保护要求。因此,企业应秉持动态、精确、客观、合法的原则做好数据的分类分级工作。

(二)隐私政策层

1.制定隐私政策。在用户注册登录前,企业需要制定隐私政策。根据《个人信息保护法》规定,企业作为个人信息处理者,在处理个人信息前,应当以显著方式、清晰易懂的语言真实、准确、完整地通过隐私政策或隐私声明向用户进行告知。告知内容可分为个人信息处理者的相关信息,个人信息处理的目的、方式等,个人行权的方式成俗以及法律、行政法规规定的其他事项。在制定隐私政策或隐私声明时,还需要注意用清晰易懂的语言和限定的篇幅进行表达,这意味着企业需考虑用户的地域、语种、阅读方便等因素,否则将面临处罚风险。例如某国外法律新闻网站,没有考虑荷兰语和法语用户对隐私政策的需求,使得应当披露给数据主体的信息不是用的清晰易懂的语言,以至于被监管机构处罚。

2.展示隐私政策。企业通过隐私政策向用户展示所收集的个人信息的范围、目的、处理方式、行权方式等,以降低用户对个人信息保护的担忧,提升用户对 App 平台的信赖,这是一种与用户良好的互动方式。在实践中,用户注册登录界面放置简明扼要的隐私政策并在注册前要求用户阅读勾选同意隐私政策。该同意需要充分知情的前提下自愿、明确地作出;同时,所展示的隐私政策需要以显著的方式、清晰易懂和不超过 300 至 500 个大号字体的语言真实、准确、完整地向用户进行告知。除了在注册环节需要展示外,还需要在用户同意后将隐私政策放置在便于用户查看的位置,建议放在 App 的个人中心页面。在用户查看时建议不得多于 3 次点击;还需要展示隐私政策的历史版本,以供用户查阅。

展示隐私政策需要注意满足知情同意、公开透明等法律原则。隐私政策内容往往过于繁杂,一般内容多达几千字,语言专业晦涩,对于普通用户阅读颇有难度,从而导致用户不阅读而直接勾选同意,使得隐私政策形同虚设,难以满足知情同意、公开透明的原则。因此,企业首先要精简内容、限制字数、扩大字体,避免多产品多场景一次性的要求用户同意隐私政策。其次,企业可以在展示时可设置一二三级目录,以便于用户整体、逐级了解隐私政策大致内容。或设置用户阅读时间要求,按照字数和正常人阅读速度来设置时间要求。最后,在展示时还需要标记重点,尤其是针对敏感个人信息、数据共享、数据跨境等涉及用户重大权益时需要通过单独弹窗、加粗等方式展示给用户。

3.更新隐私政策。企业通过 App 向用户提供产品或服务,因为 App 功能模块、企业自身性质或所有权结构、数据处理的对象发生变化、用户行权方式发生变化等情形,隐私政策需要进行更新。如果内容更改是实质性的,那么用户此前的同意将被视为撤回或无效,更新后的隐私政策需要重新取得用户的同意。同时企业还需要将隐私政策的旧版本存档,供用户查阅。因此,企业需要时刻关注可能会影响隐私政策变更的情形。即使没有发生变更的情形,建议企业定期每季度或相关法律实施时对隐私政策进行审查,保持隐私政策的最新版本,符合法律要求。

(三)权限层

企业通过 App 向用户提供产品或服务,往往需要索取部分权限以及引入第三方 SDK。由此便会引发 App 或 SDK 过度索权、未告知同意索权、频繁索权、强制索权等违法违规情形。根据《网络安全标准实践指南–移动互联网应用程序(App)系统权限申请使用指引》,对于 App 权限申请的需要满足最小必要原则,以及用户可知、不强制不捆绑、动态申请等原则。因此,在 App 正式提供给用户使用前以及使用过程中,还需要进行权限审查。

首先是与该应用组件交互所需具备的权限。例如,拍照权限,在首次索取时需要通过弹窗的方式

以清晰易懂的文字告知用户 App 的有关此权限的权限声明，用户同意后方可获取权限(android.permission.CAMERA，允许访问摄像头进行拍照)。其次,SDK 权限审查，第三方 SDK 可能包括广告、支付、统计、社交、推送,地图等类别,检查 SDK 收集信息是否符合隐私政策等。例如,位置权限,收集用于定位和追踪用户的信息，如设备 id 和位置信息;程序权限、收集用户的邮箱地址以及安装在用户设备上的应用程序列表;通讯录权限,读取短信、邮件、电话通话记录和联系人列表以及 SDK 传输数据是否以 Https 加密方式传输等。

(四)制度组织层

App 在为用户提供产品和服务时，企业要注重内部的制度组织建设。要将外部法律义务转变为内部的合规责任。要根据《网络安全法》《数据安全法》《个人信息保护法》以及梳理企业在运营 App 过程中所制定的主要制度，以便建立完善的制度的体系。因此,建议完善的制度至少需要包含公司章程即策略、管理规范和管理程序、实施流程和操作指南三级,必要时还需制定统一的表格、模板等文件,便于在适用时的规范和准确。

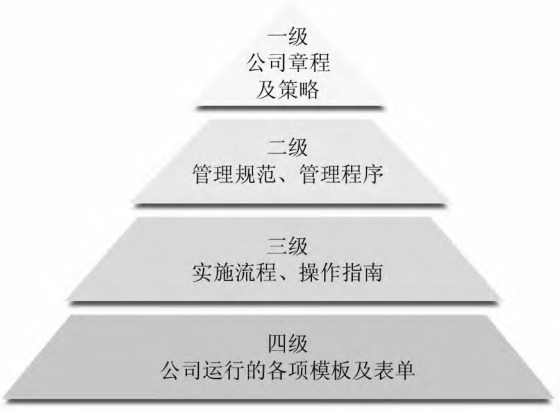

图 2　组织层级

首先是一级章程文件,企业需制定统一《公司网络安全和个人信息管理章程》等制度,明确企业网络安全与个人信息管理的总体方针、目标以及任务。建立组织架构,明确负责单位和单位职责,发挥总领性作用。其次是二级规范文件,在管理方面制定《企业个人信息管理规范》,具体可包括《企业员工个人信息保护规范》《企业供应商个人信息保护规范》《企业用户信息保护规范》《企业个人信息生命周期管理规范》《个人信息保护影响评估管理规范》《个人信息保护合规审计管理规范》等文件。在安全方面制定《企业个人信息安全规范》,具体可包括《物理和环境安全管理规范》《操作安全管理规范》《密钥密码管理规范》《安全事件管理规范》《业务连续性管理规范》等文件。三级文件在二级文件的基础上进行细化,例如《个人信息保护影响评估流程》《安全事件应急响应流程》《安全测试及安全事件监测流程》《账号权限管理流程》等。最后是四级文件,可以制定《隐私政策模板》《个人信息保护评估表》《安全事件记录表》等文件。企业建立制度体系后,还需要保留企业的制度实施记录,以备查验。

五、结语

数字经济时代 App 用户的个人信息合规风险日渐显现,本文旨在通过介绍 App 个人信息合规背景,分析企业开展 App 个人信息合规的必要性以及开展合规的难点问题,从数据层、隐私政策层、权限层、制度层等角度分析企业在开展 App 个人信息合规工作时的举措以及注意事项。近年来,App 的个人信息合规成熟度得到了较好的提升,从实践出发除此本文所提出的合规举措外,还需提升个人信息合规的数据精细度,准确识别个人信息,区分敏感个人信息、重要数据等,制度文件配套使用的图表模版。提升网络安全成熟度,网络安全是个人信息合规应有之义，即使有较为完善的个人信息合规体系,一旦发生网络安全事件将会对合规体系带来极大冲击,也会对企业的经营产生风险。最后,还需提升治理敏捷度,随着数字经济的不断发展,App 中的个人信息合规的内涵和外延也在不断发生变化,企业需要在组织措施、技术措施、法律措施等方面构建动态信息,保持进化的个人信息合规体系,实现企业个人信息合规的可持续发展。

参考文献:

[1]国务院网站[EB/OL].http://www.gov.
[2]程啸.个人信息保护法理解与适用[M].中国法制出版社:5.
[3]田宏杰.窃取 App 里个人信息的性质认定[J].人民检察,2018(7).
[4]敬力嘉.单位犯罪刑事归责中数据合规师的作为义务[J].北方法学,2021(6).
[5]国家互联网信息化办公室[EB/OL].
[6]移动互联网应用程序个人信息保护管理暂行规定(征求意见稿)[A].第 3 条.
[7]Shapiro, R. and S. Aneja (2019) "Who Owns Americans´ Personal Information and What Is It Worth?" Future Majority Report.
[8]李延舜.隐私政策在企业数据合规实践中的功能定位[J].江汉论坛,2020(10).
[9]张新宝.互联网生态"守门人"个人信息保护特别义务设置研究[J].比较法研究,2021(3).

[10]肖瑞.数字化时代企业数据合规活动的法律风险与防范[J].江苏工程职业技术学院学报,2022(1).
[11]车伟,赵申.供电企业数据盘点与数据目录构建研究[J].机电信息,2019(36).
[12]洪延青.国家安全视野中的数据分类分级保护[J].中国法律评论,2021(5).
[13]王叶刚.网络隐私政策法律调整与个人信息保护:美国实践及其启示[J].环球法律评论,2020(2).
[14]Daniel J. Solove & Woodrow Hartzog,The FTC and the New Common Law of Privacy,Columbia Law Review,Vol. 114, Issue 3,583,592-593(2014).
[15]高理想,刘昊鑫,张俊楠.App 申请和使用“可收集个人信息权限”案例分析[J].保密科学技术,2019(10).
[16]高秦伟.社会自我规制与行政法的任务[J].中国法学,2015(5).
[17]高轶峰,张楠驰.个人信息保护法解读:企业合规要求与义务履行[J].信息安全与通信保密,2021(11):9-18.
[18]吴伟光.平台组织内网络企业对个人信息保护的信义义务[J].中国法学,2021(6).
[19]李延舜.中国移动应用软件隐私政策的合规审查及完善——基于 49 例隐私政策的文本考察[J].法商研究,2019(5).

The Difficulties and Countermeasures of Enterprise Data Compliance in the Digital Economy Era ——From the Perspective of App Personal Information Compliance

GONG Zhao-qi, GONGa Zhong-qi
(Southwest University of Political Science and Law, Chongqing 401120)

Abstract: In recent years, the rapid development of the digital economy based on data resources has posed a great threat to the personal information of natural persons. Although China has established legal obligations for enterprises to protect personal information through legislation, infringement and criminal acts involving personal information often occur. This article aims to analyze the difficulties of data compliance for enterprises in the digital economy era, and find corresponding measures from four aspects: data layer, privacy policy layer, permission layer, and institutional organization layer, to ensure that the obligation of protecting personal information on the App is fulfilled while meeting legal regulatory requirements and achieving business goals, and ultimately achieve compliant processing of personal information on the App.

Keywords: digital economy; Corporate compliance; Personal informatio

（上接第 25 页）资源丰富等优势。线上线下混合式教学方式对喜欢钻研理论、追求高分的同学来说,可以反复观看理论视频学习,与老师探讨交流。而对于思维活跃、喜欢沟通的同学来说,也可以线上表达观点、积极交流,参与线下课堂活动。同时,针对学生的调查问卷反馈可知，学生对混合式教学模式是接受和认可的,并且教学效果显著,应加以推广。但也要注意线上教学资源和内容体系的构建、线下教学活动的设计、线上线下课堂活动的衔接、课程思政元素的挖掘应因地制宜,充分考虑学情,更好地培养学生自主学习能力、创新能力和应用能力。

参考文献：

[1]陆燕,薛豪娜.基于蓝墨云班课平台的《消费者行为学》课程智慧课堂教学实践与思考[J].现代商贸工业,2019(34):155-156.
[2]任碧荣,于洪深,高利梅.基于实践和创新能力培养的《消费者行为学》课程改革研究,教育现代化[J].2019(23):29-30.
[3]高明慧,向丹丹,范千喜,汪琛玉,陈文博.基于超星学习通平台混合式教学模式探究[J].科学咨询(科技·管理),2022(07):242-244.
[4]黄丽仟,玉洪荣,刘鹏.基于超星学习通平台线上教学模式与传统教学模式的比较研究[J].蛇志,2022(04):577-580.

Practice and Reflection on Blended Teaching of Consumer Behavior Based on “Nong Da Yun Shang”

FU Li-ping
(School of Economics and Management, Xinjiang Agricultural University, Urumqi 830052, Xinjiang)

Abstract: With the advancement of educational informatization, the blended online and offline teaching model is being increasingly practiced by more and more teachers due to the advantages of integrating classroom teaching and online teaching. This article is based on the “Nongda Cloud” platform and explores and practices a blended online and offline teaching model for the course of Consumer Behavior in Marketing. The results indicate that the teaching mode has achieved good teaching results, and students have experienced many advantages of blended learning mode, which has improved their understanding of knowledge points compared to traditional classrooms. In future teaching practices, it is necessary to further improve blended learning resources and teaching content, optimize blended learning practices and evaluation designs, and pay more attention to cultivating students´ humanistic sentiments.

Keywords: Consumer behavior; Blended learning; On the vast clouds; Superstar´s “One Flat Three Ends”