电商企业数据合规业务处理指引

广州市律师协会

电子商务与物流业务专业委员会　编

2024 年 4 月

目　录

引 言

近年来，数字经济方兴未艾，如雨后春笋般蓬勃发展。相继出现了元宇宙（虚拟世界，虚实相融互联网运用）、算法（从特定目的出发，对计算对象作出的具有定向性、引导性和干预性的认知计算）、区块链（去中心化）、大数据，云计算等。数字经济作为新兴经济业态，2021 年以来，上到国务院、下到江苏、河北、广东、河南、浙江、黑龙江、云南、江西、山西、福建等多地纷纷出台了促进数字经济发展的相关政策、法规等。关于数字经济的法学研究方面，近年来，学术界相继围绕着数据安全、数据合规、数据治理、数字法学等方面展开了诸多研究。其中华东政法大学马长山教授 2022 年 3 月份发表在《中国法学》上的《论数字法学》一文，直接开启了我国数字经济研究的先河。我们不禁要问：我们现阶段已经进入数字时代了吗？针对这些问题，我们试图展开以下研究探讨。

一、电商企业数据合规法律体系及基本内容

（一）电商企业数据合规法律体系

电商企业数据合规相关法律主要集中于行政法的领域，《网络安全法》、《数据安全法》和《个人信息保护法》被统称为数据合规法律的三驾马车，除此之外还包括《民法典》、《密码法》、《刑法》以及《电子商务法》中涉及个人信息与数据保护相关的法条。当然，上述法律仅是电商企业数据合规的基础，电商企业数据合规落地指引更是包含了司法解释、行政法规、各部门的规章 / 规范性文件以及行

业的技术标准。现我们就电商数据合规做了以下法规梳理：

1.法律

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国数据安全法》

（3）《中华人民共和国个人信息保护法》

（4）《中华人民共和国密码法》

（5）《中华人民共和国民法典》关于数据安全的相关条款

（6）《中华人民共和国刑法》关于数据安全的主要罪名

（7）《中华人民共和国电子商务法》关于数据安全的相关条款

2.司法解释

（1）《审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》（2020 修正）

（2）《审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》

（3）《审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（2020 修正）

（4）《非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》

（5）《检察机关办理侵犯公民个人信息案件指引》

（6）《侵犯公民个人信息刑事案件适用法律若干问题的解释》

（7）《利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》

（8）《办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》

3.行政法规

（1）《关键信息基础设施安全保护条例》

（2）《中华人民共和国电信条例》（2016 修订）

（3）《互联网信息服务管理办法》（2011 修订）

（4）《计算机信息系统安全保护条例》（2011 修订）

（5）《计算机信息网络国际联网安全保护管理办法》（2011 修订）

（6）《计算机信息网络国际联网管理暂行规定》

4.部门规章/规范性文件

（1）《网络数据安全管理条例》（征求意见稿）

（2）《互联网信息服务算法推荐管理规定》

（3）《网络信息内容生态治理规定》

（4）《网络安全审查办法》（2021 修订）

（5）《数据安全管理办法》（征求意见稿）

（6）《网络数据安全管理条例》（征求意见稿）

（7）《网络安全等级保护条例》（征求意见稿）

（8）网络安全漏洞管理规定》（征求意见稿）

（9）《直播电子商务平台管理与服务规范》（征求意见稿）

（10）《APP 违法违规收集使用个人信息行为认定方法》

（11）《常见类型移动互联网应用程序必要个人信息范围规定》

（12）《电信和互联网用户个人信息保护规定》

（13）《儿童个人信息网络保护规定》

（14）《关于全面加强电子商务领域诚信建设的指导意见》

（15）《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》

（16）《关于推进交通运输行业数据资源开放共享的实施意见》

（17）《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》

（18）《规范互联网信息服务市场秩序若干规定》

（19）《互联网个人信息安全保护指南》

（20）《关于加强网络安全和数据保护工作的指导意见》

（21）《推进综合交通运输大数据发展行动纲要(2020—2025年)》

（22）《网络交易监督管理办法》

（23）《网络直播营销管理办法（试行）》

5.国家标准/行业标准

（1）GB/T 41479-2022《信息安全技术网络数据处理安全要求》

（2）GB/T 35273-2020《信息安全技术个人信息安全规范》

（3）《信息安全技术 人脸识别数据安全要求》(征求意见稿) 等

（二）电商企业数据合规的基本内容

数据合规是指企业对数据采取的行为，从数据的收集、处理、储存，到转让、删除、销毁，都要依法执行；确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。目前，数据合

规已涉及社会多个行业和领域，其中电商是重点涉及的行业。

2021 年 6 月 10 日，我国第一部关于数据安全的法律《中华人民共和国数据安全法》公布，并于 2021 年 9 月 1 日正式施行。《数据安全法》分别从监管体系、数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任等方面，对数据处理活动进行规制，有效补充了我国《网络安全法》、《民法典》在规范数据处理活动中的不足。《数据安全法》与《网络安全法》以及《个人信息保护法》一起，全面构筑我国数据安全领域的法律框架。我国的企业数据安全合规体系的建设应围绕《数据安全法》的基本要求展开，并结合自身的行业特性、数据来源及载体的特质融入《个人信息保护法》《网络安全法》及其他法律法规的要求。

二、电商企业涉及的数据违规类型及行为表现

（一）数据安全方面

1.数据贩卖

2020 年 11 月，圆通速递被曝出有多位“内鬼”有偿租借员工账号，导致 40 万条公民个人信息被泄露事件。新京报记者从知情人士获悉，涉案的为五位圆通员工，被泄露的信息中包括发件人地址、姓名、电话以及收件人电话、姓名、地址。

2.数据垄断

（1）数字权利滥用

越来越多的 APP 出现强制授权、过度索权等数据垄断行为。美团、拼多多、携程、淘宝、飞猪、去哪儿网等平台均不同程度存在这一问

题。

（2）二选一

用网友比较通俗的话讲，就是“如果你想在天猫入驻，那你便不可在京东或其他平台上同时存在。”。

（3）大数据杀熟

经营者运用大数据收集消费者的信息，分析其消费偏好、消费习惯、收入水平等信息，将同一商品或服务以不同的价格卖给不同的消费者从而获得更多消费者剩余的行为。

（4）电商平台的刷单行为

3.数据窃取

网络爬虫相关的违法案例大增。商丘市某本科生自 2019 年 11 月起，就对淘宝实施了长达八个月的数据爬取并盗走大量用户数据。在阿里巴巴注意到这一问题前，已经有超过 11.8 亿条用户信息遭到窃取。另外的同伙利用这些信息建了 1100 个微信群，每个群 90-200 人不等，每天用机器人在群里发淘宝优惠券，赚取返利。

4.数据泄露

经常收到电话骚扰。2020 年 3 月 19 日，有用户发现 5.38 亿条微博用户信息在暗网出售，其中，1.72 亿条有账户基本信息，涉及的账号信息包括用户 ID、账号发布的微博数、粉丝数、关注数、性别、地理位置等。

（二）网络安全方面

1.滴滴下架、上市失败，因招股说明书出现国家地图、个人身份

信息。

2.《网络安全法》规定掌握超过100万用户个人信息、赴国外上市的网络平台运营者必须向网络安全审查办公室申报网络安全审查—启动审查后，经研判影响国家安全的，不允许赴国外上市。

3.分级管理。网络信息系统安全等级从低到高分为一至五级，级别越高，网络安全保障措施要求越高，相应的监管要求也会相应增强。

（三）个人信息保护方面

1.滥用人脸识别技术

（1）2021年“3.15晚会”曝光人脸识别技术滥用乱象、郭某诉杭州野生动物世界有限公司的“人脸识别第一案”等。

（2）2021年7月，杭州市市场监督管理局因某房地产公司在未征得顾客同意的前提下抓拍人脸信息，对其处以25万元人民币罚款；

（3）2021年12月，上海市市场监督管理局因某汽车公司擅自采集人脸照片，对其处以10万元人民币罚款等。

（4）《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》

2.APP审查行动

（1）2021年，工信部、网信办对应用分发平台上未明示App权限列表、用户数据收集范围以及其相关用途的，以及应用平台对App上架审核不严格、对违规App下架不及时、对App开发者身份验证不到位的情况持续进行了重点整治，并在通报中对数家应用分发平台的相关问题进行了点名批评。

（2）网信办2021年695款被通报的App中，有超过60%的App有超范围收集个人信息的情况。

（3）工信部2021年1680款被通报的App中，超过80%的App均有违规收集个人信息的情况。

（4）2021年国家网信部门通报的App类别有三方面特点：受众广泛（如新闻、视频直播类）、涉及个人信息或敏感个人信息（如求职、健康、金融类）、基础功能类App和使用关键权限的App（如应用平台类)较多;而同时具有上述多项特点的App类别被优先审查(输入法、地图导航、系统管理类）。随着专项行动的进一步开展，更多App的类别将会逐一被纳入审查范畴。

三、电商企业数据合规行政部门监管的重点和趋向

（一）数据安全方面

1.背景

《中华人民共和国数据安全法》于2021年9月1日正式实施，标志着我国数据安全监管进入了新的阶段。该法律对保障用户的数据安全和隐私权，推动电商企业的可持续发展起到了至关重要的作用。它明确了政府行政部门对电商企业的监管职责，强调了电商企业应遵守的数据安全和隐私保护义务。该法律的发布实施，为我国数据安全保护提供了重要的法律保障，也为电商企业的健康发展奠定了坚实的基础。本文将结合该法律的规定，对电商企业数据合规行政部门监管的重点和趋向进行分析。

2.监管重点

（1）数据收集和使用规范化

《中华人民共和国数据安全法》第三十二条明确规定，任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。因此，电商企业在收集和使用用户数据时，必须遵守相关法律法规，确保数据的合法性和规范性。同时，政府行政部门也将加强对电商企业数据收集和使用的监管，对违法行为进行严厉打击。

（2）数据安全保障

数据安全是电商企业必须面临的重要问题之一。《中华人民共和国数据安全法》第二十七条强调，开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。电商企业应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在数据处理过程中，电商企业应当按照规定的安全措施存储、使用、加工、传输和处理个人信息，避免数据泄露或被不当使用。政府行政部门也将对电商企业的数据安全保障措施进行监管，确保用户数据的安全性。

（3）数据跨境流动限制

随着全球化的发展，数据跨境流动变得越来越普遍。《中华人民

共和国数据安全法》对数据跨境流动进行了规定，要求电商企业在进行跨境数据流动时，必须遵守国家有关法律和法规，并按照规定的安全管理责任和措施，确保数据的安全性和保密性。政府行政部门也将对电商企业的跨境数据流动进行监管，防止数据泄露和被不当使用。

3.监管趋向

（1）强化监管力度

《中华人民共和国数据安全法》的实施，标志着我国数据安全监管进入了新的阶段。政府行政部门将加强对电商企业的监管力度，特别是对于涉及个人信息收集和使用的电商企业，将采取更加严格的措施，确保其合法性和规范性。同时，政府行政部门还将加强对电商企业数据安全的监测和预警，及时发现和处理数据安全隐患，保障用户数据的安全性。

（2）推进数据共享和利用

《中华人民共和国数据安全法》鼓励电商企业和其他组织开展数据共享和利用，促进数据的流通和开发利用。未来，政府行政部门将积极推进数据共享和利用，支持电商企业和其他组织开展合作，实现数据的互通互联和共享共用。这将有助于提高电商企业的服务质量和效率，同时也能够更好地保障用户的数据安全和隐私权。

（3）加强技术研发和应用

《中华人民共和国数据安全法》鼓励电商企业加强技术研发和应用，提高数据安全保障水平。未来，政府行政部门将加强对新技术的研究和应用，如人工智能、区块链等，为电商企业提供更加安全可靠

的技术支持。这将有助于提高电商企业的数据安全保障能力，减少数据泄露和被不当使用的风险。

（4）增强用户权益保护

《中华人民共和国数据安全法》强调了对用户权益的保护。未来，政府行政部门将加强对电商企业的监管，保障用户的知情权、选择权和隐私权。同时，政府行政部门还将加强对电商企业的社会监督，鼓励用户积极参与对电商企业的监督和评价，促进电商企业提高服务质量和管理水平。这将有助于提高用户的满意度和信任度，推动电商企业的可持续发展。

4. 结论

《中华人民共和国数据安全法》对电商企业的数据合规和行政部门监管提出了新的要求和方向。未来，政府行政部门将加强对电商企业的监管力度，推进数据共享和利用，加强技术研发和应用，增强用户权益保护等方面的工作。这将有助于提高电商企业的服务质量和效率，保障用户的数据安全和隐私权，推动电商企业的可持续发展。同时，电商企业也应当积极响应法律法规的要求和规定，加强自身管理和技术研发应用能力提升的同时也应当积极配合政府行政部门的监管工作以实现更好的发展。

（二）网络安全方面

1. 背景

《中华人民共和国网络安全法》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，是我国网络空间法治建设的重要里

程碑，标志着我国依法治网进入新阶段。该法律于2016年11月7日通过，自2017年6月1日起施行。它不仅明确了政府各部门的职责权限，强化了网络运营者的义务和责任，还加强了对个人信息的保护，维护了网络空间主权和国家安全、社会公共利益，保护了公民、法人和其他组织的合法权益。该法律的发布实施，对于保障我国网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，具有重要意义。本文将结合该法律的规定，对电商企业数据合规行政部门监管的重点和趋向进行分析。

2.监管重点

（1）数据收集与使用的合法性

根据《中华人民共和国网络安全法》第九条规定，网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。因此，电商企业在收集和使用用户数据时，必须遵循合法、正当、必要的原则，明确告知用户数据的使用目的、范围和方式，并取得用户的同意。行政部门将重点监管电商企业是否履行了告知义务，是否得到了用户的明确同意，并是否存在过度收集或使用数据的情况。

（2）数据存储与传输的安全性

电商企业应采取必要的技术和管理措施，确保数据的存储和传输安全。行政部门将关注电商企业是否采用了加密技术、访问控制等安全措施，以防止数据泄露、篡改或破坏。同时，电商企业还应定期对

数据进行备份和恢复测试，以确保在发生意外情况时能够及时恢复数据。

（3）数据出境的安全评估

《中华人民共和国网络安全法》第三十七规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。电商企业在向境外提供用户数据时，应进行安全评估，确保数据出境符合法律法规和国家安全要求。行政部门将对电商企业的数据出境活动进行监管，确保其履行了安全评估义务，并采取了必要的安全措施。

（4）网络安全防护

《中华人民共和国网络安全法》第五十五条规定，发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。国家要求电商企业应当制定网络安全事件应急预案，保证网络安全事件的及时发现、及时处置和及时报告。政府行政部门将重点关注电商企业的网络安全防护措施，包括网络基础设施的安全、网络攻击的防范和应对等，以确保电商企业的网络系统和用户数据不受安全威胁和攻击。

（5）技术研发和创新

《中华人民共和国网络安全法》第十七条规定，国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。国家鼓励电商企业在网络安全领域进行技术研发和创新。政府行政部门将关注电商企业在网络安全方面的技术研发和创新情况，包括新技术、新方法的研发和应用等，以推动电子商务行业的整体发展和进步。

3.监管趋向

（1）严格的执法和处罚力度

随着网络安全形势的日益严峻，政府行政部门将会更加重视电商企业的数据合规问题，并采取更加严格的执法和处罚措施。对于违反《中华人民共和国网络安全法》及相关法规的电商企业，政府行政部门将会依法进行处罚，包括罚款、责令改正、停业整顿等措施。这将有效震慑违法企业，促使电商行业更加重视数据合规问题。

（2）注重数据保护技术创新和应用

随着技术的发展和进步，政府行政部门将会更加注重电商企业在数据保护方面的技术创新和应用。鼓励电商企业采用新技术、新方法来保护用户数据的安全，如区块链技术、人工智能等。同时，政府行政部门还将加强与企业的合作，共同研发和推广数据保护技术和解决方案，提高电商行业的整体网络安全水平。

（3）注重用户教育和意识提升

用户教育和意识提升是维护网络安全的重要一环。政府行政部门

将会更加注重电商企业在提升用户教育和意识方面的措施，包括开展网络安全宣传周活动、发布网络安全知识手册等。通过增强用户的网络安全意识和防范能力，降低用户遭受网络攻击的风险。

（4）注重行业自律和合作

政府行政部门将会更加注重电商行业的自律和合作。通过制定行业规范、建立行业协会等方式，促进电商企业之间的协作和交流。同时，政府行政部门还将加强与电商企业的合作，共同推动电子商务行业的健康发展。

（5）注重数据安全风险评估和防范

政府行政部门将会更加注重电商企业的数据安全风险评估和防范工作。要求电商企业定期进行数据安全风险评估，及时发现和解决潜在的安全风险。同时，政府行政部门还将加强数据安全风险的监测和预警，及时发布风险提示和应对措施，保障电商企业和用户数据的安全。

从《中华人民共和国网络安全法》的角度来看，政府行政部门将来对电商企业数据合规的监管趋向可能会表现在更加严格的执法和处罚力度、更加注重数据保护技术创新和应用、更加注重跨境数据流动的管理、更加注重用户教育和意识提升以及更加注重行业自律和合作等方面。这些措施将有助于保障电子商务市场的安全稳定运行，维护用户的合法权益和国家安全。

4. 结论

《中华人民共和国网络安全法》是我国网络领域的基础性法律，

旨在保护网络空间安全，维护网络用户的合法权益。该法律对政府、企业和个人都提出了相应的要求和责任，为我国的网络安全工作提供了法律保障。未来，政府行政部门将加强对网络的监管力度，推进网络安全工作的开展。企业作为网络运营的主体，也应当积极响应法律法规的要求和规定，加强自身管理和技术研发应用能力提升的同时也应当积极配合政府行政部门的监管工作以实现更好的发展。

对于电商企业来说，网络安全法的重要性不言而喻。电商企业应当遵守网络安全法的规定，采取必要的技术和管理措施，保障网络运营的安全性和稳定性，保护用户的个人信息安全。同时，也应当积极配合政府行政部门的监管工作，加强自身管理和技术研发应用能力提升的同时也应当积极配合政府行政部门的监管工作以实现更好的发展。

综上所述，《中华人民共和国网络安全法》的实施对于保障网络空间安全，维护网络用户的合法权益具有重要的意义。电商企业应当积极响应法律法规的要求和规定，加强自身管理和技术研发应用能力提升的同时也应当积极配合政府行政部门的监管工作以实现更好的发展。

（三）个人信息保护方面

1. 背景

《中华人民共和国个人信息保护法》是我国第一部个人信息保护方面的专门法律，旨在保护公民个人信息权益，规范个人信息处理活动，促进个人信息合理利用。该法律于 2021 年 8 月 20 日通过，自

2021 年 11 月 1 日起施行。它明确了个人信息处理者的义务和责任，对个人信息权益的保护提供了法律保障。该法律的发布实施，标志着我国个人信息保护工作进入了一个新的阶段，对于保护公民个人信息安全，维护社会稳定和国家安全具有重要意义。本文将结合该法律的规定，对电商企业数据合规行政部门监管的重点和趋向进行分析。

2.监管重点

（1）个人信息收集和使用

《中华人民共和国个人信息保护法》第五条规定，处理个人信息应当遵循合法、正当、必要和诚信原则,不得通过误导、欺诈、胁迫等方式处理个人信息。因此，电商企业收集和使用个人信息应当合法、正当、必要，并遵循诚信原则。政府行政部门将重点关注电商企业在收集和使用个人信息方面的行为，包括个人信息的种类、数量、目的、方式和范围等，以及电商企业是否按照法律规定的方式和范围使用个人信息。

（2）个人信息保护政策

《中华人民共和国个人信息保护法》第四条规定，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。电商企业应制定个人信息保护政策，明确收集、使用、加工、传输、存储、公开等个人信息处理活动的规则和程序。政府行政部门将重点关注电商企业的个人信息保护政策是否符合法律规定，以及是否明确规定了个人

信息处理活动的规则和程序。

（3）信息安全和隐私保护

《中华人民共和国个人信息保护法》要求电商企业采取技术措施和其他必要措施，确保其收集、存储、使用和加工的个人信息安全、准确、完整、及时，防止信息泄露、篡改或者毁损。政府行政部门将重点关注电商企业的信息安全和隐私保护措施是否符合法律规定，以及是否能够有效地保护个人信息的安全和隐私。

（4）跨境数据流动管理

随着电子商务的全球化发展，电商企业的跨境数据流动变得越来越普遍。《中华人民共和国个人信息保护法》第三十八条规定，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当依照本法第四十条的规定通过国家网信部门组织的安全评估、按照国家网信部门的规定经专业机构进行个人信息保护认证以及按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务。因此，政府行政部门要求电商企业在跨境数据流动时，应当按照规定进行安全评估，并采取必要的安全措施。政府行政部门将重点关注电商企业的跨境数据流动情况，包括出境数据的种类、数量、目的和来源等，以及电商企业是否采取了必要的安全措施来保护个人信息的安全和隐私。

（5）用户权益保护

《中华人民共和国个人信息保护法》强调对个人权益的保护。《中华人民共和国个人信息保护法》第四十四条规定，个人对其个人信息

的处理享有知情权、决定权,有权限制或者拒绝他人对其个人信息进行处理;法律、行政法规另有规定的除外。政府行政部门将重点关注电商企业在处理个人信息时是否尊重用户的权益,包括用户对个人信息的查询、复制、更正、删除等权利是否得到保障。

（6）内部管理和责任追究

《中华人民共和国个人信息保护法》第五十八条规定要求电商企业建立健全个人信息保护合规制度体系,成立主要由外部成员组成的独立机构对个人信息保护情况进行监督,平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务,对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者,停止提供服务。政府行政部门将重点关注电商企业内部管理和责任追究机制是否健全,以及是否能够及时发现和处理个人信息泄露等安全事件。

3.监管趋向

（1）强化法律执行和处罚力度

随着个人隐私保护意识的增强,政府可能会更加严格地执行《个人信息保护法》,对违法电商企业进行处罚。这些处罚可能包括罚款、责令改正、停业整顿等,以遏制电商企业的不法行为,进一步规范电商市场的数据合规管理。

（2）完善数据安全和隐私保护制度

政府可能会进一步强化对电商企业数据安全和隐私保护的监管,要求电商企业采取更完善的数据保护措施,确保用户个人信息的保密性、完整性和可用性。同时,政府还将加强对电商企业数据安全事件

的监测和预警，及时发现和处理数据泄露等安全事件。

（3）重视跨境数据流动的管理

随着电子商务的全球化发展，跨境数据流动将变得更加普遍。政府可能会更加重视电商企业的跨境数据流动管理，制定更加严格的法规和标准来规范电商企业的跨境数据流动行为。同时，政府还将加强与其他国家和地区的合作，共同打击跨境网络犯罪活动，维护国家安全和用户隐私。

（4）注重用户权益保护

政府可能会更加注重电商企业在处理个人信息时对用户权益的保护。未来，可能会明确用户对个人信息的查询、复制、更正、删除等权利，并要求电商企业及时告知用户相关信息，并按照用户的要求进行处理。同时，政府还将加强对电商企业的监督和检查，确保其遵守相关法律法规和保障用户权益。

（5）加强社会监督和公众参与

政府可能会更加注重社会监督和公众参与在电商企业数据合规监管中的作用。未来，可能会鼓励社会各界参与对电商企业的监督和检查工作，并建立相关的投诉举报机制。同时，政府还将加强与公众的沟通和互动及时回应公众关切和解决投诉问题共同推动电商市场的健康发展。

4.结论

从《中华人民共和国个人信息保护法》的角度来看，未来政府行政部门对电商企业数据合规的监管趋向将更加严格和全面。政府将加

强对电商企业的监督和检查，注重个人信息的安全和隐私保护，以及跨境数据流动的管理。同时，政府还将注重用户权益的保护，鼓励电商企业进行技术研发和创新应用，并加强社会监督和公众参与的作用，共同推动电商市场的健康发展。这些措施将有助于保障用户个人信息的安全和隐私，维护电商市场的公平竞争秩序，促进电商行业的可持续发展。

四、电商企业数据合规着力点及开展途径

（一）数据资产盘点+数据识别

1.数据全生命周期合规要求

（1）制度建立

建立健全全流程数据安全管理制度，落实数据安全保护责任，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施保障数据安全。

（2）风险监测

对数据处理活动中出现的缺陷、漏洞等风险，要采取补救措施；发生数据安全事件要按规定上报。

（3）风险评估

对数据处理活动定期开展风险评估并上报风评报告。

（4）收集使用

任何组织、个人收集数据必须采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

（5）数据交易

数据服务商或交易机构，要提供并说明数据来源证据，要审核相关人员身份并留存记录。

（6）存储加工

委托他人存储、加工或提供政务数据，要先审批，并做好监督。

（7）配合调查

要求依法配合公安、安全等部门进行犯罪调查。境外执法机构要调取存储在中国的数据，须先审核。

（8）审批与监督

委托他人建设、维护系统，或涉及存储、加工数据，应当经过严格的批准程序，并监督受托方、数据接收方履行相应的数据安全保护义务。

2.数据合法性基础梳理、论证

（1）同意

同意是最为大众所熟知、常见的合法性基础。许多企业喜欢在收集、处理个人信息前获取数据主体的同意，并认为自己已经满足了合法性基础的要求。但是，“同意”真的可以作为万金油吗？或者换句话说，你的“同意”真的有效吗？在 EDPB 发布的指南 05/2020 中对“同意”进行了详细的说明和介绍，构成一个有效的“同意”，需要满足“自由给予”、“具体”、“充分告知”、“明确意愿表示”四个要素，同时需要符合“随时撤回”、“提供证明”两个要求。大致来说，数据控制者如果想要将“同意”作为合法性基础，需要首先评估用户如果撤回同意，是否会对其有不利的影响（例如服务质量降低等），数据主体与自己是否存在不平等的关系（例如学校和学生之间、

雇主和雇员之间，如果数据控制者希望依赖于“同意”，则需要证明拒绝同意不会产生不利的后果）。在评估结束后，需要设计“同意”的交互方式及文本。在交互方式上确保不会出现捆绑同意（将“同意”和“提供服务”的请求进行打包，不同意则不提供服务）和一揽子获取同意（多个“同意”请求进行打包），同时提供可以供消费者随时撤回同意的渠道。

综上所述，“同意”作为合法性基础，一方面由于需要满足“随时撤回”，并不适用于需要长期、稳定的数据处理，另一方面，由于“自由给予”的相关要求，同意适用的场景被大大的限制，此外，它对数据控制者提出了更多的合规责任（有效性评估、撤回渠道、同意记录保留、响应更多的数据主体权利）。

（2）合同所必须

由于对于同意的使用有比较高的限制，合同所必需是十分重要的一项合法性基础。“合同所必需”即如果缺少指定个人信息，数据控制者将无法订立或履行合同/服务。例如，缺少了银行帐号则无法转账汇款。如果数据控制者想要将“合同所必需”作为合法性基础，首先需要确保所需数据确实为必须的，不然会出现捆绑同意（将“同意”和“提供服务”的请求进行打包，不同意则不提供服务）。此外，当合同/服务停止后，需要立刻停止对数据的处理，包括存储。此时，如果数据控制者还想继续处理个人信息，需要寻找另外的合法性基础。例如，数据控制者的法律责任、数据控制者的合法利益。欧洲议会要求数据控制者处理活动的每一目的只能依靠一项合法性基础，且需要对每项合法性基础的使用进行说明。那么如何避免监管机构认定企业宣称合法性基础全部都是基于用户的“同意”呢？目前有两种主流实践。第一种，在交互上进行区分：张毅老师曾预测，“欧盟在线服务为了避免

其在合法性基础上的混淆，非常可能在用户界面的设计上不会全部要求用户勾选。即便是勾选，相信这种隐私协议的提示也会从“我已同意”变成“我已审阅”在2021年的今天，这种预测已经变成了一种实践。第二种，在法律文书上进行区分：不少企业在隐私政策中会以表格或文本。

当下，许多企业习惯使用“合同所必需”作为“为了给您提供更好的服务”及“防止欺诈”的合法性基础，并将这两项编入基础合同条款中的一部分。、

3.数据识别

关于重要数据的定义目前在理论界、实务届仍然属于“哥特巴赫猜想”，目前来说其定义的边界依然不够明确，具有很强的“口袋”特征。较为准确的定义来源于中央网络安全和信息化委员会办公室、工业和信息化部开展“个人信息和重要数据安全专项调查”，在中国互联网协会的《专项调查问题列表与答复》（“答复”）重要数据是指：不涉及国家秘密，但如果泄露、窃取、篡改、毁损、丢失和非法使用可能危害国家安全、国计民生、公共利益的未公开数据，包括:（1）地理、自然资源、重要物资储备等数据;（2）基因、生物特征、疾病等数据;（3）宏观统计等重要经济数据；（4）网络信息系统的缺陷、漏洞、防范措施等数据;（5）人群导航位置、大型设备目标位置和移动数据；（6）法律法规规定的其他重要数据。

4.数据流转

（1）共同处理

共同处理，是指两个及以上的处理者共同决定个人信息的处理目的和处理方式。

（2）委托

委托，是由委托人决定个人信息的处理目的和处理方式，受托人受托处理。

（3）转移

转移，是因为合并、分立、解散等原因，将个人信息转移给他人，自己不再保留。

（4）提供

提供，是指一方将个人信息提供给另一方，双方各自继续处理个人信息。

（5）公开

（二）合规组织架构和人员设置

1.个人信息保护负责人

个人信息保护法规定，处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

如何理解设立这一职位的必要性？首先，数字时代个人信息处理行为无处不在，但政府的监管不可能无处不在，因此设立个人信息保护负责人可以强化企业自我监管，从而弥补政府监管的不足、促进平台治理；第二，个人信息保护负责人能够作为连接纽带，推动个人信息保护的协同治理，为用户提供直接与企业进行沟通的渠道；第三，个人信息保护负责人也可以连接政府和企业，具有一定制度功能。

个人信息有不同的种类，以后可能需要根据具体的种类和级别来确立设立负责人的标准。建议采取一些激励措施，鼓励没有达到信息

处理规模的企业自愿设立，同时公共机构也应当设立个人信息保护负责人。

在个人信息保护负责人的资质问题上，目前有关资质条件的规定比较宽泛，实际上应该对其文史哲知识、法律经济技术等专业能力进行考量，一般由内部人员担任。同时，由于个人信息保护负责人需接受全过程监督，其自身的个人信息也应得到适当保护，在公开负责人相关信息时，面向社会、面向政府、面向企业内部提供的内容应有所区分。比如，面向社会时不应公开负责人的重要信息，主要公布邮箱、电话等。

2.网络安全等级保护工作责任人

网络安全等级保护工作责任人是甲方单位一把手。首先，《中华人民共和国网络安全法》明确表示，每个单位应确定网络安全负责人，落实网络安全保护责任，其中提到的按照网络安全等级保护制度的要求，履行安全保护义务。那么，网络安全等级保护制度里又是如何描述呢？在《网络安全等级保护制度基本要求》中相关描述指出单位应成立网络安全领导小组，那么网络安全的主体责任就在这个小组上了，领导小组组长不是单位一把手，也得是一把手指派的人员，那一把手依然有责任。在网信办或是网安进行安全检查时，发现的问题是有依据对一把手进行问责的。在《中华人民共和国网络安全法》第三十一条又提出要进行关键信息基础设施保护。同样，《中华人民共和国数据安全法》中也提出要求单位对收集和产生的数据及数据安全负责，又适用关键信息基础设施条例和《中华人民共和国网络安全法》，那

么关键信息基础设施条例是什么呢？《关键信息基础设施安全保护条例》是旨在建立专门保护制度，明确各方责任，提出保障促进措施，保障关键信息基础设施安全及维护网络安全，根据《中华人民共和国网络安全法》制定的条例，于 2021 年 4 月 27 日，经国务院第 133 次常务会议通过。2021 年 7 月 30 日，国务院总理李克强签署中华人民共和国国务院令第 745 号公布，自 2021 年 9 月 1 日起施行。在《关键信息基础设施安全保护条例》第十三条指出运营者的主要负责人对关键信息基础设施安全保护负总责。所以，我国用法令明确规定网络安全“主要负责人负总责”实行一把手负责制。而网络安全与数据安全是息息相关，分不开的，所以数据安全责任也是同样如此。

3.网络安全管理负责人

根据《中华人民共和国网络安全法》的规定，网络运营者应确定网络安全负责人，关键信息基础设施运营者应设置专门安全管理机构和安全管理负责人。2018 年 11 月 26 日，工信部公布了对数家公司的信息网络安全检查情况，并对其中 7 家进行行政处罚，其中 2 家企业因未确定网络安全负责人被处罚，责令改正。网络安全负责人是一个什么样的岗位？对于不同类型的企业来说，应如何设置网络安全负责人以满足相应的法律要求？《网络安全法》没有对网络安全负责人的岗位和职责进行具体规定，仅笼统规定网络运营者应确定网络安全负责人，关键信息基础设施的运营者应设置专门安全管理机构和安全管理负责人，并对违反这一要求的网络运营者和关键信息基础设施运营者设置了行政处罚规则，包括对直接负责的主管人员进行罚款，从

而确定了单位和个人均需承担责任的双规处罚机制。网络运营者的主要负责人应有充分的动力指定合格的网络安全管理负责人，以确保企业的网络安全合规，减小企业的合规风险及自身的法律风险。

4.数据安全责任人（若以经营为目的收集重要数据）

2019 年 5 月，网信办制定的《数据安全管理办法（征求意见稿）》（下称“《网络安全法（征）》”）17 条规定，“网络运营者以经营为目的收集重要数据或个人敏感信息的，应当明确数据安全责任人。”。对此，企业要判断自身是否要设置数据安全责任人的标准有三个，第一为判断自身是否为网络运营者，第二为是否以经营为目的，第三为是否收集重要数据或收集个人敏感信息。企业可以根据自身业务范围和场景看是否在日常经营过程中收集《网络安全法（征）》规定的重要数据，同时，判断自身业务是否以收集用户的个人敏感信息为支撑。若有，就需要设置数据安全责任人。

5.专门安全管理机构负责人（适用 CIIO）

《网络安全法》第三十四条第（一）款要求关键信息基础设施运营者应当设置专门安全管理机构及安全管理负责人。《关键信息基础设施安全保护条例》第十四条、第十五条在此基础上，进一步明确了 CIIO 安全管理机构的职责。公安部门处罚事由多为未设置网络专门安全管理机构、安全管理负责人；未对关键岗位人员进行安全背景审查；未定期对从业人员进行网络安全教育、技术培训和技能考核；未制定网络安全事件应急预案并定期进行演练等。说明对于 CIIO 来说，设置专门安全管理机构是十分重要且必要，也是 CIIO 履行网络安全保

护义务的首要任务。如何组建专门安全管理机构，目前行业内并无成熟的做法。

根据《网络安全法》、《关键信息基础设施保护条例》等相关法律法规的规定，CIIO 是 CII 保护的主体单位，负责 CII 的运行、管理，履行网络安全保护义务，而专门安全管理机构则是 CIIO 内部专门负责本单位关键信息基础设施保护工作，履行关键信息基础设施保护职责义务的主要实体部门。

（三）内部合规制度流程设计

1.内部管理制度和操作规程

一方面，在数据合规领域，企业应重点关注技术、管理、内控等部门合规规范的执行与遵守。另一方面，企业数据合规涉及个人信息保护和重要数据保护等合规规范，企业合规部门需要与业务部门结合企业使用和处理数据的实际情况，合作制定和修改相关的业务合规流程，实现法律监管与业务发展之间的平衡。

2.违规操作的内部惩戒机制

由于惩戒是对劳动者的一种惩罚，借鉴其他类型的惩戒规则，也应当遵循正当程序原则。程序正当不仅包括惩戒规则制定的正当程序，也包括惩戒措施实施的正当程序。对于前者，应当符合我国《劳动合同法》第 4 条的规定。对于后者，雇主在实施惩戒时，应告诉雇员惩戒的事由和理由，应给予雇员陈述和申辩的机会，可以考虑借鉴《劳动合同法》第 43 条有关雇主单方面解除劳动合同时，将理由事先通知工会的规定，要求企业在存在工会时，将惩戒事由和理由事先通知

工会。

（四）数据安全管控及保障设计

1.数据分类分级管理

数据分类分级的基本原则是数据分类管理和数据分级保护。

从企业经营维度来看，我们可以将企业运行数据分为用户相关数据、企业业务数据、经营管理相关数据、系统运行数据和安全数据。用户相关数据是指企业在为客户提供产品或服务的过程中向个人或组织采集的数据信息，以及企业在开展业务过程中产生的应归属于用户群体的数据信息，主要包括个人信息（个人自然信息、个人身份鉴别信息等）、组织信息（组织基本情况、信用信息等）。企业业务数据是指企业在生产或经营过程中形成的与企业自身相关的数据信息。我们可以参考企业业务所属行业对产生的数据进行分类分级，也要注意结合企业自身的业务特点进行细分，如产品数据、合同协议等。经营管理相关数据是指企业在日常经营和管理过程中采集到的各类型数据，这些数据既包括内部产生的数据，也包括外部采集的数据，如公司经营战略、财务数据、并购投资及债务融资信息、人力资源数据等。系统运行数据和安全数据显示了网络和信息系统的日常运维情况，包括系统配置参数、网络设备的安全管理监测数据、日志数据和网络安全漏洞信息等。除上述四个维度之外，企业数据划分还可以继续向下拓展，进一步做二级子类、三级子类细分，如参照《基础电信企业数据分类分级方法》中的企业数据分类范例，用户数据可继续细分为用户身份相关类数据、用户服务内容相关数据及其衍生的信息数据、

用户信息统计分析类数据。

2.采取加密、去标识化等安全技术措施合理确定操作权限

企业为了维护数据安全，可以通过采取一些加密措施或者通过去标识化的安全技术措施来确定不同人员的操作权限，从而达到保护数据安全。同时有些数据可以设定保存期限，定期开展渗透性测试与攻防演练。

（五）产品用户权利保护设计

1.隐私保护设计方案/同意机制设计方案

隐私保护设计的核心：架构。单一架构下的信息提供和信息服务，信任和约束都不稳定，越界问题也就不可避免，信息泄密是迟早的事，调整架构成为必要。而采用多元架构，在多元实体之间建立正向相互促进、反向相互制约、全程监管的机制，从不同维度解决信息提供、加工、服务、信任传递、权力监管等问题成为首选。多元架构为你保障信息的“不可见不可用、可用不可见、可用可见”提供架构支撑。

2.个人行权响应与行权机制

在为个人信息主体的赋予法定权利的同时，个保法第 50 条亦明确要求个人信息处理者需要建立便捷的个人行使权利的申请受理和处理机制，即为个人信息主体行使其权利创造条件。从实践角度来看，由于个保法第 17 条要求企业在处理个人信息前，向个人信息主体告知个人信息处理者的名称及联系方式，企业通常会采用通过制定并发布隐私政策的方式来履行该义务，许多企业直接使用隐私政策中所告知的联系方式作为个人信息主体联系企业并行使权利的渠道。具体而

言，主要的公开渠道是企业设立的电子邮箱、联系电话及企业办公场所的邮寄地址，个人信息主体通过向以上渠道发送具体的行权要求来达成行使权利的目的。然而，在实践中，这种单向的信息传达机制往往会在收到行权要求后出现各种问题。

首先，由于缺少统一的行权入口和标准的行权范式，行权信息呈现分散化、碎片化、非标准化的特征，企业需要从多个渠道中接收并识别信息，增加前期信息收集的时间成本。此外，收集到的信息内可能存在着大量垃圾广告、恶意投诉等无效信息，以及语义模糊或不合理的行权要求，这些信息与个人信息主体合理的行权请求混杂在一起，对企业向个人信息主体行权要求做出的正常响应形成干扰。企业需要在信息流中分辨出个人信息主体提出的行权请求，并及时作出记录。在这个检验并筛选的过程中，不仅需要付出人力成本、增加前端处理时间，同时还面临着信息发现不及时或信息被遗漏等潜在隐患。

因此对于企业而言，可以考虑建立统一的行权入口并启用针对性的权利响应平台，打通不同渠道、汇集行权请求，以应对行权信息碎片化的问题，及时高效地收集行权信息。

3.投诉/举报/反馈通道

当用户遇到电商企业数据方面的问题，企业应当保证电商客服的在线和处理。

（六）与第三方合作数据保护设计

1.委托合同中的数据保护条款

对于委托合同中的数据保护条款应当甄别交易主体及其角色、识

别数据处理情形、甄别企业在数据处理活动中的权责三、梳理各交易文件的关系。

2.专门的数据处理协议

数据处理协议，专指企业与专业数据服务商，或者说数据控制者与数据处理者之间的协议，一般是主合同数据服务协议的从合同，它针对数据服务中关于数据处理的特别事项进行详细约定。订立数据处理协议时应当注意：明确数据处理协议双方的法律关系、隐私政策、设置安全性条款、明确对信息的存储区域、删除、更正、销毁或归还数据。

3.采购网络产品和服务网络安全审查

以运营者为直接规制对象、以审查采购合同为手段确保 CII 供应链安全。根据新办法的规定，采购网络产品和服务时，需要履行网络安全审查申报的义务主体是 CII 的运营者，而不是网络产品和服务的提供者。同时，根据新办法规定，运营者应通过采购文件、协议等要求产品和服务提供者配合网络安全审查，配合的内容包括：a)产品和服务提供者承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，b)产品和服务提供者承诺无正当理由不中断产品供应或必要的技术支持服务等。我们理解，新办法通过要求在采购文件、协议载明 a)和 b)两项内容的方式，为产品和服务提供者设定了义务，实际上是以审查采购合同为手段确保 CII 相关产品、服务供应链的安全。此外，我们需要注意运营者申报网络安全审查与签订采购合同的先后关系。

4.第三方供应商背景审查与服务监测

首先，在与第三方建立业务关系之前，企业应在关注第三方供应商的生产规模、资金实力、资质认证和行业地位以外，进一步对管理层信用情况、供应商的合规状况、上下游关系及其他潜在警示信号等方面进行信息收集，以全面评估第三方关系。其次，在建立业务关系后，企业应以风险为导向，定期或不定期对第三方供应商开展更深入的背景尽职调查，并有效评估和掌握其潜在的运营或合规相关的风险及信息的做法，则是企业预防并有效控制潜在风险的重要防控屏障，而且使企业避免如因第三方资质造假等引发的质量缺陷，或因企业内外部的欺诈、贪腐或制裁问题引发的经济损失和声誉损害。

（七）数据合规评估机制设计

1.个人信息保护影响评估 重要数据处理活动风险评估 数据出境风险自评估

根据《个人信息保护法》第 55 条规定，个人信息处理者在向境外提供个人信息前需进行个人信息保护影响评估即“PIA”。

评估实施过程中采用的基本评估方法，主要为以下三种：访谈、检查、测试。

数据安全风险评估是做好重要数据和核心数据监管与保护工作的重要一环。《数据安全法》要求“重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估”。《工业和信息化领域数据安全管理办法（试行）》提出了“工业和信息化领域重要数据和核心数据处理者应当自行或委托第三方评估机构，每年对其数据处理活动至

少开展一次风险评估，及时整改风险问题，并向本地区行业监管部门报送风险评估报告”的具体细化要求。

根据《数据出境安全评估办法》第5条，数据处理者在向网信办申报数据出境安全评估前，应当开展数据出境风险自评估即“自评估”。数据出境风险自评估是要基于对企业数据出境的业务、信息系统、数据资产等情况的了解，评估维度包含了数据处理者的情况、境外接收方的情况，在数据传输风险的评估上，主要是通过对信息系统、数据链路、接收后的数据安全等情况进行评价。

2.赴境外上市的数据处理者对数据安全自评估

赴境外上市的企业可能因日常业务运营或上市活动而触发数据出境安全评估义务，而《办法（征求意见稿）》在现行数据保护法律法规以及配套规则的基础上进一步细化了申报数据出境安全评估的条件与流程，明确要求重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险。就数据出境安全评估，《办法（征求意见稿）》的核心要求如下：

（1）适用主体——数据处理者

《办法（征求意见稿）》要求，“数据处理者”将境内所涉数据向境外提供的场景下，应当进行安全评估。

（2）适用范围——境外

依据国内法律法规如《出境入境管理法》对于“境外”的定义，我们理解，赴境外上市企业向国外国家或者地区以及我国的港澳台地区提供在中国境内收集的重要数据和依法应进行安全评估的个人信

息，均需适用《办法（征求意见稿）》的规定开展安全评估。

（3）评估程序——自评或申报

《办法（征求意见稿）》规定，数据处理者向境外提供任何数据均需开展数据出境风险自评估，若公司向境外提供数据且符合《办法（征求意见稿）》第四条规定的以下五种情形之一的，还需通过所在地省级网信部门向国家网信部门申报数据出境安全评估：(i)关键信息基础设施的运营者收集和产生的个人信息和重要数据；(ii)出境数据中包含重要数据；(iii)处理个人信息达到一百万人的个人信息处理者向境外提供个人信息；(iv)累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息；(v)国家网信部门规定的其他需要申报数据出境安全评估的情形。

2. 赴国外上市的关基运营者对采购活动及互联网平台运营者对安全性及掌握个人信息数据量自评估

2022 年实施的《网络安全审查办法》将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查，并明确掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须向网络安全审查办公室申报网络安全审查。根据审查实际需要，增加证监会作为网络安全审查工作机制成员单位，同时完善国家安全风险评估因素等内容。

运营者申报网络安全审查，应当提交以下材料：（一）申报书；（二）关于影响或可能影响国家安全的分析报告；（三）采购文件、协议、拟签订的合同或拟提交的 IPO 材料等；（四）网络安全审查工

作需要的其他材料。

（八）内外部政策声明设计

1.隐私声明

隐私声明，是跨境电商网站所有者为确保自身及其客户行使权利履行义务，从而保障双方共同利益而发布的法律文件。隐私声明主要用于说明商家将如何收集、处理、存储、共享、使用和保护客户通过与网站的交互收集到的个人数据信息，例如姓名、电子邮件地址、IP地址、会话活动和支付细节等等。一份全面高效的隐私政策既是商家对客户数据信息安全的承诺，也可以防范潜在的数据安全诉讼，同时有助于客户建立对商家网站和业务的信心。

那么一份好的隐私声明应该如何制定，又应该包含哪些内容呢？首先，商家需要了解你的海外市场所在国家的相关隐私立法，遵照相关法律规定制定自己的隐私政策。其次，一份清晰有效的隐私政策至少应涵盖如下方面的内容：（1）商家对“个人数据”的定义是什么？商家将收集什么样的数据信息？隐私政策通常会告知用户可用来直接识别你身份的数据(如你的姓名)属于个人数据，不能用来直接识别你的身份但可通过合理推断间接识别你身份的数据(如你的设备序列号)也是个人数据。隐私政策还应详细说明商家从访问者和客户收集的信息的类型，并告知为什么要收集这些数据以及如何使用用户的数据信息。例如，如果你正在收集他们电子邮件地址，你的隐私策略应该明确地说明这一点，并说明收集电子邮件地址是为了通讯需要。(2)客户在此享有的隐私权有哪些？商家通过隐私政策告知客户其隐私

权会获得尊重，比如其具有获知、访问、更正、传输、限制处理和删除个人数据的权利和能力。承诺当客户选择行使这些隐私权时，客户不会因此受到商家的区别对待，客户有权获得商家的标准程度的服务质量。隐私政策应该包含一个部分，详细说明客户如何查看所收集的信息，以及如何更改或删除这些信息。商家应该赋予客户更改、编辑或删除个人数据，以及选择不与商家共享他们的数据的权利。隐私政策中还需详细说明如果商家将业务出售或合并到另一家公司将会发生什么。此条款被称为“Business Transfer”条款，它应该说明如果业务的所有权发生变化将会发生什么，以及你的公司将采取哪些步骤来转移客户数据的所有权。（3）商家将如何使用客户的数据信息？跨境商家通常应该披露会出于以下目的使用个人数据：为服务提供支持、处理客户的交易、与客户沟通、实施安全和防欺诈措施以及遵守法律等。商家也可能在经客户同意并有合法的法律依据时将个人数据用于其他用途。收集必要的个人数据来为商家的服务提供支持，收集的数据可能用于产品或服务的改进、用于审计或数据分析等内部目的或用于故障诊断等。商家需要收集客户的姓名、购买内容和付款信息等数据处理交易。商家需要个人数据用于回复客户的讯息、就客户的交易或账号与客户联系、推销商家的产品和服务、提供个性化客户服务、提供其他相关信息或请求客户提供信息或反馈等。商家为了保护客户、员工和自身，防止损失和预防欺诈，预先筛选或扫描上传内容中的潜在非法内容，包括儿童不法虐待内容等。商家为了遵守相关法律使用客户个人数据信息，例如履行税务或申报义务，遵守合法的政府要求、

执行法院命令、传票等。（4）商家可能对客户个人数据进行共享吗？如果商家可能与其附属公司或服务提供商、合作伙伴等第三方共享客户的个人数据，隐私政策中应该清晰告知客户。例如商家可能聘请第三方作为其服务提供商，代表商家处理或储存与客户使用商家的服务和向客户交付产品相关的个人数据。服务提供商有义务按照本隐私政策的规定和商家的指示处理个人数据。未经允许服务提供商不能将商家共享的个人数据用于其自己的目的，完成服务要求后须按协议要求处理这些数据。商家可以按照客户的指示或在客户同意的情况下与其他人共享客户的个人数据，来为客户提供更好的服务。（5）如何对个人数据，包括儿童数据，提供保护？跨境商家应该在隐私政策中详细披露如何使用管理性、技术性和物理性保护措施来保护客户的个人数据，同时会将个人数据的性质、数据的处理以及面临的威胁纳入考虑。商家应告知客户其深知保护儿童个人数据的重要性，因此会实施额外程序和保护措施来帮助保障儿童个人数据的安全，以及如果商家得知某个孩子的个人数据是在未经适当授权的情况下收集的，会尽快将其删除。（6）Cookie 政策隐私政策应披露其网站、在线服务、互动应用程序和广告可能会使用“Cookie”和其他技术，比如网站信标。包括用于支持商家系统的出入网络流量，用于帮助检测错误而生成流量的通信 Cookie；为了提供客户访问或请求的特定功能或服务而必须设置的绝对必要 cookie 以及其他 Cookie。如果客户不接受使用 Cookie，商家应提供停用 Cookie 的选项和方法。如果商家提供了无法使用 Cookie 的选项，请告知客户无法获得的某些网站功能。（7）

如有隐私问题，应联系谁隐私政策应该提供负责维护隐私程序的工作人员或数据保护官的联系信息，并考虑创建一个特殊的地址。告知客户在大多数情况下，实质性咨询会在几天之内得到答复。（8）隐私政策的生效日期和更新日期商家一定要及时更新隐私政策，记录所做的任何更改，并始终在最后一次更新时显示。

2.数据保护声明等

数据保护声明应当包含定义、法律依据、目的、信息种类、数据收集来源、数据保存期限、安全措施、用户权利、声明的更改等内容。

结语

本指引旨在解决关于电商企业数据合规的基本问题，力求给该行业提供规范指引。本指引从电商企业数据合规的法律体系、基本内容为切入点，将现有我国关于数据合规应当遵循的法律法规做了一个罗列指引，同时指出行业内关于数据合规违规的主要类型包括数据安全、网络安全两大板块，对我国行政部门关于数据合规监管的方向和趋势做了重点阐述，最后提出了关于数据合规的着力点和开展途径，给电商企业数据合规提供了一个全面详实的规范指引，当然随着数据经济的发展，数据合规的问题也是层出不穷，限于编者专业水平有限，对于很多新兴业态方面的数据合规问题尚研究不深，故本文仍有很多有待改进之处，也请各位同仁提出宝贵建议，在此一并表示感谢。