数据保护新规逐条解读·企业合规热点事件解析

数据保护合规指引与规则解析

—第2版—

刘新宇◎主编

根据《数据安全法》
《个人信息保护法》全新修订

Data Protection
Compliance Guidelines and Rule Analysis

中国法制出版社
CHINA LEGAL PUBLISHING HOUSE

数据保护合规指引与规则解析

—第2版—

主编：刘新宇

编委会人员：吴豪雳　葛　舒　冯中杰　卢佳宏

宋海新　陈嘉伟　张倩文　周士尊

Data Protection

Compliance Guidelines and Rule Analysis

中国法制出版社

CHINA LEGAL PUBLISHING HOUSE

序　言

数据商业利用与个人信息保护之间存在的对立，无疑是数字社会发展中遇到的最大矛盾。合理的个人信息保护是数据商业交易不反噬个人私领域的基本保障和前提，而数据的自由流动与个人信息的正当使用则是数字社会健康发展的基础。这两者相辅相成、和谐发展方能带来数字社会的繁荣。如何平衡数据商业利用与个人信息保护之间的关系，最大效用地利用数据与信息，且能有效保护数据主体的最大权益，将是数据治理中的永恒核心议题。

在信息化趋势下，网络空间内安全威胁的范围不断扩大，具体表现形态也纷繁多样，网络安全形势愈发严峻。在此背景下的数据处理，尤其是其规模的不断扩大，也带来了更多的网络空间安全问题。如何通过高水平的立法应对网络安全威胁，保护关键信息基础设施和公民个人信息安全，维护国家利益和公民合法权益，进而推动我国网络空间国际治理能力的发展，亦成为在网络安全领域立法需回应的问题。

最近十年，“科技寡头”的快速扩张，时常会引发用户们对于自身的个人信息和数据是否能得到合理保护的担心，与个人数据保护相关的事件和诉讼案件开始频繁涌现。这些与个人数据相关的议题，不断占据舆论热点。其中揭示的现实问题是：个人用户数据权利意识愈发强烈，企业的数据合规也愈发重要。这也使得企业个人数据的合规能力，正在和企业的商业信誉愈发紧密地捆绑在一起。在可见的未来，企业的数据合规将和企业名誉、利益甚至命运息息相关。甚至可以说，一个企业的信息合规能力，在未来会成为决定其综合实力的重要影响因素。

刘新宇博士等作者前瞻且深刻地认识到，在数据商业运用广泛铺开的21世纪，数据本身的开放性、共享性和无形性，决定了法律人不仅会在学理层面遇到信息权利建构等各方面的挑战，而且更会让信息控制者和法律从业者，在实务的数据交易和数据运用中面对各种棘手的难题。面对这些问题，不仅立法者需要跳出传统法律体系的框架，面对新情况即时调整规范；法律从业者和个人信息持有者，也需要即时适应数据权利保护不断流变的法

律框架，把握规范发展的脉络，甚至做出具有前瞻性的合规调整。

本书作为数据保护实务指引，凝聚了作者在长期法律研究和实务工作中的所见、所思、所得，紧跟数据保护热点、难点和重点，对数据合规相关问题的分析深入浅出，并从数据保护全生命周期的角度提出了具体的实务操作建议，具有较强的可行性，能够帮助读者在大数据时代，更好地应对新兴的数据合规挑战。这本书的亮点还在于收录了作者对数据保护相关新规的解析，方便读者在近两年数据保护新规不断出台的情况下，第一时间掌握新规的要点、难点，并为读者有效落实新规的要求提供了针对性的指导。

本书的几位作者均是在数据保护领域深耕多年的专家，熟悉各类数据商业应用的场景，对数据合规有着充分而深刻的理解。其中新宇跟我攻读博士期间便参与了跟我主持的国家社科基金重大课题“大数据时代个人数据保护与数据权利体系研究”相关的学术研究。其博士学位论文也是以《数据权利构建及其交易规则研究》为题，较为深入地研究了大数据时代下数据权属的认定、交易规则和数据权利构建等相关问题。可喜的是，他去年还在核心期刊上发表了《大数据时代数据权属分析及其体系构建》一文，指出目前以用户为中心的个人信息“绝对保护”框架，已经无法有效地调整经营者和用户之间的复杂关系；而现代社会正愈发倾向于一种动态化的双向保护方式，以平衡个人信息权益与经营者数据资产权益。可以看出，他在执业之余，一直在数据法律领域坚持学习与研究。

本书作者尽管付出了艰辛努力，但对相关法律规章的解读还可更为细致些，对于案例的分析还可更为全面些，对一些基本概念或术语的介绍还可更加深入些。但瑕不掩瑜，本书丰富而系统的法律规章梳理，全面而富有针对性的条文解读以及对于典型案例的分析等，无论是对于数据企业，还是对于相关法律从业者，都会带来一定助益；也相信这本书对于企业数据合规体系在未来的构建，能够带来实际帮助。感动于作者在繁忙的实务工作中，不忘学习与研究！更期待新宇博士无论在实践业务，还是在学理知识上，继续努力与进步！

彭诚信
上海交通大学凯原法学院副院长、教授
2021 年 6 月于凯原法学院

目 录

第一部分

我国数据保护现状概述

一、引言

当下，相关技术及市场的快速发展深刻改变着现有的生产和生活方式，正引发思维方式和社会形态的剧烈变革。数据有价，数据商品化的实现将数据使用和保护的平衡推到了信息化时代的台前，如何平衡数据的保护和利用并促进数据的流通成为新的关注点。一方面，民众权利意识的提升亟待法律的回应；而另一方面，企业和政府使用信息给民众带来巨大便利的现实，又不断提醒着我们，法律应当谨慎把控数据保护的力度，保障信息的流通自由。

现如今，数据，尤其是个人信息，对于实现风险控制、风险定价、精准营销、产品开发和战略分析等发挥着越来越重要的作用。但与此同时，其带来的风险也是不能忽视的。近年来，境内外数据安全事件频发，无论是信息泄露、某支付软件年度账单、转卖内部数据权限等重大数据安全事件，还是各类个人信息买卖案件、App 个人信息侵权事件，在使社会公众信息安全和财产安全面临威胁的同时，也引发了政府和公众对数据安全的思考。

2020 年 5 月 28 日通过的《民法典》将个人信息的相关规则写入民事立法中，确立了个人信息相关权利的法律地位及性质。而在此之前，2017 年 6 月 1 日，《网络安全法》正式实施，其作为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，不仅是我国网络空间法治建设的重要里程碑，也就数据和个人信息合规提出了许多框架性的要求。《网络安全法》实施以来，各类配套法规、规章和标准化文件不断出台。尤其是 2019 年以来，数据保护相关规范的出台速度明显加快，规则体系的框架已越发清晰，对应的合规要求也逐渐落向实处。《数据安全法》于 2021 年 6 月 10 日发布，2021 年 9 月 1 日正式施行，成为我国数据安全领域的基本法。《个人信息保护法》于 2021 年 8 月 20 日发布，2021 年 11 月 1 日正式施行，标志着我国个人信息保护领域基本法的落地，也标志着我国数据保护方面基本立法框架的形成。

随着我国政府数据安全意识不断加强以及个人信息主体自身权利意识的逐渐觉醒，做好数据保护已经成为面对着监管要求和舆情压力的企业在规划发展战略和开展日常运营工作的过程中不可忽视的重要环节。

二、数据保护立法现状

在现代社会治理中，将数据治理与个人信息保护放到更加重要的地位上已经成为国际社会的广泛共识。于我国而言，尽管聚焦个人信息保护的专门法律——《个人信息保护法》于2021年8月20日方正式通过，但与数据保护相关的条文早在多年以前便开始散见于法律、司法解释以及相关的部门规范性文件中，其具体的发展脉络梳理如下：

（一）非刑事法律、法规、规章层面

1. 时间发展脉络

2012年3月15日，《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第20号）正式施行，其明确规定，除法律、行政法规另有规定外“能够单独或者与其他信息结合识别用户的信息”的收集、使用、提供必须“经用户同意”。就此，“可识别性”成为认定个人信息的核心标准，个人信息保护的客体开始逐渐明晰。

2012年12月28日，《全国人民代表大会常务委员会关于加强网络信息保护的决定》正式发布生效，明确了国家对于网络信息安全的保护，强调了公民个人信息收集过程中的合法、正当、必要原则以及防止个人信息泄露的义务，国家越发重视对于个人的网络信息保护。

随后的两三年间，征信、工信、消费者保护等领域的立法都将个人信息保护纳入了相应的法律文本中，如《征信业管理条例》、《电信和互联网用户个人信息保护规定》（工业和信息化部令第24号）、《消费者权益保护法》等。

2017年6月1日，《网络安全法》正式实施。作为我国网络和数据安全框架性的立法，它标志着我国网络安全保护相关的众多制度要求开始逐步建

立。在安全等级保护方面，《网络安全等级保护条例（征求意见稿）》、《网络安全等级保护测评机构管理办法》（公信安〔2018〕765号）等规定相继发布或生效；在关键信息基础设施保护方面，《关键信息基础设施安全保护条例（征求意见稿）》发布；在数据出境方面，《个人信息和重要数据出境安全评估办法（修订稿）》《个人信息出境安全评估办法（征求意见稿）》（以下简称《个人信息出境办法（征求意见稿）》）等规定的制定，标志着数据跨境传输方面的制度要求逐渐完善。此外，国家网信办还于2019年5月28日发布了《数据安全管理办法（征求意见稿）》，以应对《数据安全法》出台前的数据安全保护问题。

伴随着《网络安全法》的施行和相关监管实践活动的开展，在积累了充分监管经验的前提下，更具针对性的数据立法开始大量发布。如2019年10月1日起施行的《儿童个人信息网络保护规定》（国家互联网信息办公室令第4号），对于儿童个人信息的保护采取了更加严格的手段，并基于儿童个人信息保护的特殊性对儿童个人信息保护进行了专门的规定。而针对一些App过度收集用户个人信息，隐私条款不完善等问题，国家网信办、工信部、公安部、国家市场监管总局四部委也于同年11月28日联合发布了《App违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191号）。该文件既为监管部门认定App违法违规收集使用个人信息行为提供了参考，也为App运营者自查自纠和网民社会监督提供了具体的实务指引。

2. 地方立法情况

我国不同地区的网络条件及技术能力存在较大差异，不同地区数据保护情况可能存在区别。实践中，部分地方政府也尝试通过制定地方法规的方式对数据处理活动进行规范。

例如，天津市网信办发布的《天津市数据安全管理办法（暂行）》于2019年8月1日正式施行，开启了地方监管机关开展监管探索的尝试。此后，《重庆市政务数据资源管理暂行办法》《贵州省大数据安全保障条例》等地方规定也相继出台。可以预见的是，地方基于区域特点进行数据方面针对性立法的趋势仍将延续。

3. 行业立法情况

随着新业务的出现和发展，数据保护亦在不同行业的立法中表现出专业化和精细化特征。

例如金融行业2011年5月1日发布的《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》（银发〔2011〕17号），此后，《银行业金融机构数据治理指引》（银保监发〔2018〕22号）、《中国人民银行金融消费者权益保护实施办法》（中国人民银行令〔2020〕第5号）相继发布，对金融行业数据保护提出了具体的规范要求。

再如网约车行业和物流行业，《寄递服务用户个人信息安全管理规定》《网络预约出租汽车经营服务管理暂行办法（2019修正）》等行业立法相继发布，其中涉及大量旨在规制行业中数据收集和使用等的具体条文。

这类行业立法进一步充实了数据保护的相关规则体系，对具体行业的数据保护提供了更具针对性的规范要求。

（二）刑事层面

1. 相关刑事法律

在立法层面，我国对数据和个人信息的保护存在着“刑法先行”的立法模式。

1997年修订的《刑法》规定了破坏计算机信息系统罪，侵入他人计算机删除、修改、增加数据信息的行为开始受到刑事处罚。

2009年2月28日，《刑法修正案（七）》正式施行，其增设了出售、非法提供公民个人信息罪，非法获取计算机信息系统数据、非法控制计算机信息系统罪等罪名。《刑法修正案（七）》不仅采用刑事手段规制金融机构等单位工作人员提供、获取、交易个人信息的行为，也首次将侵入非国有计算机仅获取数据的行为也纳入了刑事规制的范围之内，对于他人计算机信息的删改行为不再成为入罪的必须要件，《刑法》对数据保护的力度得以加强。

2015年施行的《刑法修正案（九）》则修改了《刑法》第253条之一，放宽了犯罪主体的限制，提升了法定最高刑的刑期，并规定对于在履行职责

或者提供服务过程中获得的公民个人信息，非法出售或提供的行为，可以从重处罚。修改后，“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”被整合为“侵犯公民个人信息罪”。同时，《刑法修正案（九）》也增设了非法侵入计算机信息系统罪、破坏计算机信息系统罪等罪名的单位犯罪规定。

2. 相关司法解释

最高人民法院、最高人民检察院和公安部出台了一系列同数据保护相关的司法解释，以指导相关司法案件的侦查、检察和审判。

2013 年 4 月 23 日，《最高人民法院、最高人民检察院、公安部关于依法惩处侵害公民个人信息犯罪活动的通知》（公通字〔2013〕12 号）要求坚决打击侵害公民个人信息犯罪活动。该通知明确规定侵害公民信息犯罪的定罪量刑应当综合考量非法出售、提供、获取个人信息的次数、数量、手段和牟利数额等因素，与此同时，该文件对于具有可识别性的个人信息进行了较为细致的列举，如姓名、年龄、有效证件号码、婚姻状况、工作单位、学历、履历等。

2014 年 10 月 10 日，《最高人民法院关于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》（法释〔2014〕11 号）正式施行，全方位地确定了利用信息网络侵害个人信息案件的审理流程与审判要点。2021 年 1 月 1 日，修订后的《最高人民法院关于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》正式生效，进一步完善了相关审判流程和审判要点。

2017 年 6 月 1 日，《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（法释〔2017〕10 号，以下简称《侵犯公民个人信息刑事案件解释》）正式施行。该司法解释对侵犯公民个人信息罪的构成要件、量刑标准和具体法律适用问题进行了系统性的规定。

其后两年内，《最高人民检察院检察机关办理侵犯公民个人信息案件指引》（高检发侦监字〔2018〕13 号）和《最高人民法院、最高人民检察院关于办理非法利用信息网络、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》（法释〔2019〕15 号，以下简称《网络犯罪解释》）对于侵

犯公民个人信息案件的具体构成要件，明确了更为细致的证据审查要求和更加清晰的定罪量刑标准。

（三）国家标准、指南层面

我国数据相关立法的一个鲜明特征便在于，通过大量的国家标准、指南为企业开展数据合规安排提供参考。国家标准在制定程序上相对更为灵活，更贴近不断发展变化的数据活动的实践需要。

2013 年 2 月 1 日，《信息安全技术　公共及商用服务信息系统个人信息保护指南》（GB/Z 28828 - 2012）正式实施。这是我国关于个人信息保护的首个国家标准，该文件确立了信息处理的基本原则（目的明确原则、最少够用原则、公开告知原则等），明确将个人信息区分为个人敏感信息和一般个人信息，并区别规制。

2017 年 12 月 29 日，全国信息安全标准化技术委员会（以下简称信安标委）发布了《信息安全技术　个人信息安全规范》（GB/T 35273 - 2017，以下简称《个人信息安全规范（2017）》）。该标准系我国个人信息保护领域最重要、影响最为广泛的国家标准，其对于个人信息的相关名词进行了系统化、专业化的定义，并对于个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为进行了规制。其后，根据实践中个人信息收集、使用的变化及《个人信息安全规范（2017）》在实施过程中出现的问题，信安标委分别于 2019 年 2 月 1 日、6 月 25 日及 10 月 22 日发布了《信息安全技术　个人信息安全规范（草案）》（以下简称《个人信息安全规范（草案）》）和两次征求意见稿，不断根据监管实践中发现的用户画像、个人生物识别信息收集等相关新问题对规范的内容进行调整，并于 2020 年 3 月 7 日发布了《信息安全技术　个人信息安全规范》（GBT 25273 - 2020，以下简称《个人信息安全规范》）正式稿。

在《网络安全法》确立的具体制度方面，许多制度框架亦是通过国家标准来搭建和完善的。例如，在网络安全等级保护方面，《信息安全技术　网络安全等级保护基本要求》（GB/T 22239 - 2019）、《信息安全技术　网络安全等级保护测评要求》（GB/T 28448 - 2019）、《信息安全技术　网络安全

等级保护实施指南》（GB/T 25058－2019）、《信息安全技术　网络安全等级保护安全设计技术要求》（GB/T 25070－2019）等多部国家标准均已实施，以全力推动我国网络安全等级保护制度从“等保1.0”向“等保2.0”时代演进。再如，在《网络安全法》和《个人信息安全规范》搭建的一系列收集、使用个人信息制度的基础上，《信息安全技术　个人信息去标识化指南》（GB/T 37964－2019，以下简称《个人信息去标识化指南》）、《信息安全技术　大数据安全管理指南》（GB/T 37973－2019，以下简称《大数据安全管理指南》）、《信息安全技术　个人信息安全影响评估指南》（GB/T 39335－2020，以下简称《个人信息安全影响评估指南》）等配套国家标准也相继生效或发布，为数据安全和个人信息保护提供了更加详细和具体的指引。

（四）数据保护相关法律、法规、规章、规范性文件及国家标准汇总

当前我国数据保护相关的重要法律、法规、规章、规范性文件及国家标准参见下表：

序号	文件名称	发布机构	生效时间	法律/文件状态
A. 数据保护相关的重要法律、法规、规章及规范性文件				
1	《消费者权益保护法》第14条、第29条、第50条、第56条	全国人大常委会	2014年3月15日	现行有效
2	《刑法修正案（七）》	全国人大常委会	2009年2月28日	现行有效
	《刑法修正案（九）》第17条、第28条		2015年11月1日	
3	《网络安全法》	全国人大常委会	2017年6月1日	现行有效
4	《电子商务法》第5条、第23条、第25条、第32条	全国人大常委会	2019年1月1日	现行有效
5	《密码法》	全国人大常委会	2020年1月1日	现行有效
6	《民法典》第111条、第1032～1039条	全国人大	2021年1月1日	现行有效
7	《数据安全法》	全国人大常委会	2021年9月1日	现行有效
8	《个人信息保护法》	全国人大常委会	2021年11月1日	已发布，即将生效

续表

序号	文件名称	发布机构	生效时间	法律/文件状态
9	《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》	最高人民法院、最高人民检察院	2017 年 6 月 1 日	现行有效
10	《最高人民法院、最高人民检察院关于办理非法利用信息网络、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》	最高人民法院、最高人民检察院	2019 年 11 月 1 日	现行有效
11	《最高人民法院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》	最高人民法院	2021 年 8 月 1 日	现行有效
12	《最高人民法院关于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》	最高人民法院	2021 年 1 月 1 日	现行有效
13	《征信业管理条例》	国务院	2013 年 3 月 15 日	现行有效
14	《电信和互联网用户个人信息保护规定》	工信部	2013 年 9 月 1 日	现行有效
15	《儿童个人信息保护规定》	国家网信办	2019 年 10 月 1 日	现行有效
16	《App 违法违规收集使用个人信息行为认定方法》	国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局办公厅	2019 年 11 月 28 日	现行有效
17	《工业数据分类分级指南（试行）》	工信部	2020 年 2 月 27 日	现行有效
18	《网络安全审查办法》	国家网信办	2020 年 6 月 1 日	现行有效
19	《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》	工信部	2020 年 7 月 22 日	现行有效

续表

序号	文件名称	发布机构	生效时间	法律/文件状态
20	《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》	公安部	2020年9月22日	现行有效
21	《中国人民银行金融消费者权益保护实施办法》	中国人民银行	2020年11月1日	现行有效
22	《常见类型移动互联网应用程序必要个人信息范围规定》（以下简称《个人信息范围规定》）	国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局	2021年5月1日	现行有效
23	《关键信息基础设施安全保护条例》	国务院	2021年9月1日	现行有效
24	《汽车数据安全管理若干规定（试行）》	国家互联网信息办公室、中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国交通运输部	2021年10月1日	即将生效
25	《网络安全等级保护条例（征求意见稿）》	公安部	2018年6月27日	正式版未发布，未生效
26	《数据安全管理办法（征求意见稿）》	国家网信办	2019年5月28日	正式版未发布，未生效
27	《个人信息出境办法（征求意见稿）》	国家网信办	2019年6月13日	正式版未发布，未生效
28	《网络安全漏洞管理规定（征求意见稿）》	工信部	2019年6月18日	正式版未发布，未生效
29	《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）》（以下简称《App保护规定（征求意见稿）》）	工信部	2021年4月26日	正式版未发布，未生效