

作者：

贾维恒

weihengjia@qinlilegal.com

曲晓琨

seanqu@qinlilegal.com

杨哲榆

eryang@qinlilegal.com

如欲垂询更多信息，请联络
上海勤理律师事务所专业人士：

叶伟文

资深全球顾问
patyipqinli@qinlilegal.com

陈朕

codychen@qinlilegal.com

费亚力

alexfischer@qinlilegal.com

贾维恒

weihengjia@qinlilegal.com

陆易

clu@qinlilegal.com

马骋

roma@qinlilegal.com

宋姣琳

jolsong@qinlilegal.com

葛向阳

xyge@qinlilegal.com

韩桢

zhenhan@qinlilegal.com

刘萍

liuping@qinlilegal.com

林泽军

jasonlinzj@qinlilegal.com

马锋

jasonma@qinlilegal.com

蒋利众

lzjiang@qinlilegal.com

开启数据合规新篇章——《数据安全法》要点解读

《数据安全法》于2021年6月10日，经中华人民共和国第十三届全国人民代表大会常务委员会表决通过，并将自2021年9月1日起施行。《数据安全法》是围绕网络、数据、信息安全主题的系列法律之一，与《网络安全法》以及将要出台的《个人信息保护法》构成该领域的三大基础性法律。《数据安全法》尤其确立了数据安全的大原则，以及国家党政机构的管理和处罚权限。

一、《数据安全法》要点梳理和解读

（一）适用范围

《数据安全法》第2条规定了该法的适用范围是“在中华人民共和国境内开展数据处理活动及其安全监管”。也就是说该法的主要调整对象是行为，即“数据处理活动”以及政府部门对数据处理活动的“安全监管”的行为。该法并不是一个对数据民事权利义务进行规范的法律。换言之，任何组织或个人，在中国境内进行数据处理活动的，都必须服从《数据安全法》的规范。同时，与近期出台的涉及国家安全系列法律一脉相承，《数据安全法》第2条明确规定，中国将依法追究损害中国国家安全、公共利益等的境外数据处理行为的法律责任。

《数据安全法》也广泛地界定了“数据处理”的范围，定义了数据处理为“包括数据的收集、存储、使用、加工、传输、提供、公开等”。该定义中列举了已知且常见的数据处理行为，并使用了“包括”、“等”定义方式，为国家将来进一步通过司法或行政解释的方式，扩大该法的适用范围，预留了空间。

（二）监管机构及其职权

《数据安全法》第 5、6 条规定了数据安全监管机构及其职权。

- a. **中央国家安全领导机构**负责国家数据安全工作的决策和议事协调，建立国家数据安全工作协调机制等。国家通过立法，将数据安全和网络安全上升到国家安全的高度。目前，负责中国国家安全的最高领导机构是中共中央国家安全委员会。
- b. **行业主管部门**承担本行业、本领域数据安全监管职责。根据该授权规定，各行业主管部门可以进一步制定符合各行业情况的数据安全监管细则。比如，工信部可以对互联网、汽车行业的数据安全监管制定细则。
- c. **公安机关、国家安全机关**在其相应职责范围内承担数据安全监管职责。根据《国家安全法》的规定，公安机关、国家安全机关有权依法搜集涉及国家安全的情报信息，依法行使侦查、拘留、预审和执行逮捕以及法律规定的其他职权。目前公安机关已经设立了网络安全监察、网络安全保卫等部门，对网络进行监督管理。
- d. **国家网信部门**负责统筹协调**网络数据安全**和相关监管工作。目前国家网信部门有“中共中央网络安全和信息化委员会办公室”和“国家互联网信息办公室”，为一个机构两块牌子，直属于中共中央和国务院。

（三）数据安全制度

1. 数据分类分级保护制度

《数据安全法》第 21 条规定国家建立数据分类分级保护制度。其基本原则是根据其重要程度和一旦遭受侵害而造成的危害程度进行分类保护。根据该法规定，可以理解为数据将被分为三类进行保护和管理：（1）国家核心数据，（2）重要数据，（3）一般数据。对于国家核心数据的范围和定义，《数据安全法》只给出了一个简单大原则，没有明确任何机构有权或将会就“国家核心数据”进行认定、出具更有操作性的目录等，我们推测核心数据的目录有可能在“重要数据目录”中进行规定。

《数据安全法》明确了国家将协调出台“重要数据目录”，并要求对于重要数据进行重点保护。我们推测后续会有进一步的法规就重要数据的管理方式和保护条件，进行进一步的明确。

虽然《数据安全法》没有提及一般数据，但根据法律的解读，除了国家核心数据和重要数据以外的数据，应当属于一般数据。

2. 数据安全审查制度

《数据安全法》第24条规定国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查，且依法作出的安全审查决定为最终决定。但《数据安全法》未规定数据安全审查的具体规则和适用范围。本条更是一个授权条款，授权数据监管机构可以进行国家安全审查。企业是否需要取得任何事先或事后审批，或需要采取任何行动来规避风险尚不明确。

3. 数据出口管制

《数据安全法》第25条规定国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制，《数据安全法》的该等规定与《出口管制法》的规定形成了衔接。《出口管制法》规定了对相关货物、技术、服务等物项，包括物项相关的技术资料等数据，的出口管制要求。据此，如果待出境数据落入出口管制清单，数据出境还应根据《出口管制法》获得国务院、中央军事委员会出口管理部门的许可。

(四) 数据安全保护义务

1. 数据安全保护

《数据安全法》第27条规定，开展数据处理活动应当：

- a. 依法建立健全**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。
- b. 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，履行数据安全保护义务。
- c. 此外，**重要数据的处理者**应当明确**数据安全负责人和管理机构**，落实数据安全保护责任。

关于网络数据处理所适用的网络安全等级保护，《数据安全法》该条规定与《网络安全法》第21条关于网络运营者应当按照网络安全等级保护制度的要求履行相关安全保护义务的规定相呼应。公安部曾发布《网络安全等级保护条例（征求意见稿）》公开征求意见，依据该条例，网络根据重要程度及一旦遭到侵害而造成的危害程度分为五个安全保护等级，高等级的网络应采取高等级的安全保护措施；且第二级以上的网络，还应当通过专家评审、行业主管部门核准，以及公安机关备案。《网络安全等级保护条例》有待正式出台。另外，需要关注的是，国家标准化管理委员会已经出台了《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 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）等相关标准，形成了网络安全等级保护的标准体系。

2.数据安全风险及安全事件应对

《数据安全法》第 29 条规定开展数据处理活动应当：

- a. 加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；
- b. 发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

3.风险评估

《数据安全法》第 30 条规定**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**，并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

4.数据出境管理

《数据安全法》第 31 条规定：

- a. **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**重要数据**的出境安全管理，适用《网络安全法》的规定；
- b. **其他数据处理者**在中华人民共和国境内运营中收集和产生的**重要数据**的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

《网络安全法》第 37 条要求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重要数据（以及个人信息）出境须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。国家网信部门关于重要数据出境安全评估的办法曾公开征求意见，尚待出台。

此外，《数据安全法》第 36 条还规定，非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。

（五）法律责任

《数据安全法》第 45 条规定了开展数据处理活动的组织、个人不履行相关数据安全保护义务（《数据安全法》第 27 条、29 条、30 条规定的义务）所应承担的法律责任；第 46 条规定了对于违反数据出境安全管理规定（《数据安全法》第 31 条）向境外提供重要数据所应承担的法律责任；《数据安全法》第 48 条规定了对于违反规定（《数据安全法》第 36 条规定）未经主管机关批准向境外的司法或执法机构提供数据所应承担的法律责任。该等法律责任，视违法行为情节和造成后果的严重程度而定，包括：

- a. 对企业责令改正、给予警告、处以罚款，以及**责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照**。

b. 对企业直接负责的主管人员和其他直接责任人员处以罚款。

值得注意的是，对违反国家核心数据管理制度，危害国家主权、安全和发展利益的，以及违反数据出境安全管理规定，情节严重的，对企业的罚款可达到一千万元。

除上述处罚外，《数据安全法》也同时规定了行为构成犯罪，违反治安管理或给他人造成损害的应承担相应法律责任。但《数据安全法》本身并未详细规定刑事责任、治安管理处罚以及民事责任的具体适用情形，对此应依据《刑法》、《治安管理处罚法》和《民法典》等规定视个案具体情况进行判断。

二、我们的观察

一方面，《数据安全法》确立了系统的数据安全治理的基本框架，为国家管理数据安全提供了原则性法律基础。另一方面，《数据安全法》涉及的数据安全相关的关键问题，如重要数据界定、数据安全出境管理等问题，仍有待相关细则进一步明确。

关于重要数据界定问题，目前《数据安全法》以及《网络安全法》未对重要数据的概念作出规定，后续根据《数据安全法》的规定，国家将出台重要数据目录。对于重要数据的概念、范围等，国家互联网信息办公室曾发布《数据安全管理办法（征求意见稿）》、《个人信息和重要数据出境安全评估办法（征求意见稿）》，全国信息安全标准化技术委员会曾发布《信息安全技术 数据出境安全评估指南（征求意见稿）》尝试进行界定。此外，全国信息安全标准化技术委员会还拟编写《信息安全技术 重要数据识别指南》对重要数据的识别制定标准。重要数据的概念、范围、目录等有待国家后续出台相关文件进行明确。

关于数据出境安全管理问题，就重要数据而言，《数据安全法》较《网络安全法》增加了关于除关键信息基础设施运营者以外的其他数据处理者控制的（在中华人民共和国境内收集和产生的，下同）重要数据的出境管理规定，管理办法由国家网信部门会同国务院有关部门制定。基于《网络安全法》等的规定，国家互联网信息办公室曾发布《个人信息和重要数据出境安全评估办法（征求意见稿）》，全国信息安全标准化技术委员会曾发布《信息安全技术 数据出境安全评估指南（征求意见稿）》尝试对重要数据出境安全评估制定规则。数据出境安全管理，尤其是数据出境安全评估的具体规则有待相关正式文件进行确定。

数据被广泛认为是下个时代国家和经济组织的核心竞争力。国家安全、个人隐私、数据权属等问题不断涌现。作为数据安全大原则的法律规范也势在必行，《数据安全法》出台后，《个人信息保护法》以及相关行政法规、规章、标准等文件亦将密集出台，有鉴于此，所有企业及相关人员均必须对数据合规工作及早着手，追踪法律法规的出台，梳理企业目前的数据处理流程，完善数据处理合规措施。

本文由上海勤理律师事务所为本所中国大陆及香港之客户及员工编制，内容只供信息提示与参考之用，并不代表本所对相关事项的全部理解，也不构成任何法律建议。在您就本文中涉及的事项做出商业决策前，请务必咨询合格的专业顾问。如欲垂询有关本文的资料或其它意见，请联络：

叶伟文

资深全球顾问
patyipqinli@qinlilegal.com

陈朕

codychen@qinlilegal.com

陆易

cllu@qinlilegal.com

葛向阳

xyge@qinlilegal.com

林泽军

jasonlinzj@qinlilegal.com

费亚力

alexfischer@qinlilegal.com

马骋

roma@qinlilegal.com

韩桢

zhenhan@qinlilegal.com

马锋

jasonma@qinlilegal.com

贾维恒

weihengjia@qinlilegal.com

宋姣琳

jolsong@qinlilegal.com

刘萍

liuping@qinlilegal.com

蒋利众

lzjiang@qinlilegal.com

关于上海勤理律师事务所

上海勤理律师事务所是 Deloitte Legal 全球网络成员。上海勤理律师事务所编制、发布了本《法律评论》系列刊物，对较为常见的法律问题以及最新进展进行介绍与评论。上海勤理律师事务所定期与政府部门及权威机关就新近出现的法律问题及相关发展进行沟通及商议，并针对相关问题撰写深入评析，提供专业意见。如欲垂询，请联络：

上海勤理律师事务所

中国上海市延安东路 222 号
外滩中心 15 楼第 5 单元
邮政编码：200002
电话：+86 21 6141 1718
传真：+86 21 6335 0003
www.qinlilegal.com

上海勤理律师事务所是 Deloitte Legal 全球网络成员。

如欲索取本文的电子版或更改收件人信息，请电邮至 inquiries@qinlilegal.com 或传真至 +86 21 6335 0003。

本文件中所含乃一般性信息，故此，并不构成上海勤理律师事务所（商号：“勤理”）、其人员及代理人提供任何专业建议或服务。在做出任何可能影响自身、自身财务或业务的决策或采取任何相关行动前，请咨询合格的专业顾问。本文件中所含资料及信息乃以其原貌提供，上海勤理律师事务所并未对该等文件所含资料或信息做出明示或暗示的陈述或保证。在不限制上述规定的前提下，上海勤理律师事务所不保证该等文件所含资料或信息没有错误或达到了任何特定的实施或质量标准。上海勤理律师事务所明确否认所有暗示的或其它保证，包括但不限于适销性、所有权、适合特定目的、不侵权、兼容性、安全性和准确性的保证。上海勤理律师事务所、其人员及代理人不对任何方提起的或其产生的由于其依赖本文件所致的或与本文件相关的任何损失或索赔承担责任。

上海勤理律师事务所是 Deloitte Legal 全球网络成员。

© 2021 上海勤理律师事务所 版权所有 保留一切权利