中国企业数据保护白皮书（2017年）

数据中心联盟

2018年1月

版权声明

本白皮书起草单位：中国信息通信研究院、北京谷安天下科技有限公司、北京天空卫士网络安全技术有限公司。

本白皮书起草人：孙明俊、李海英、王蕴韬、曹峰、杨婕、石霖、龚文全、陈伟、郭秀元、杨明非、陆明。

目录

一.前言

随着云计算、大数据、移动互联网、人工智能等信息通信技术蓬勃发展，以数据为核心的智能化革命，正在成为产业转型升级的新动力和新引擎。我国政府高度重视数据在新常态中推动国家现代化建设的基础性、战略性作用。2017 年 12 月 8 日，习近平总书记在“中共中央政治局就实施国家大数据战略进行第二次集体学习”时强调,“要加快完善数字基础设施，推进数据资源整合和开放共享，保障数据安全,加快建设数字中国,更好服务我国经济社会发展和人民生活改善。”在新的需求模式下，特别是数据已经成为国家基础性资源的背景下，数据保护这一议题已经被提升到前所未有的战略高度。

为推进我国数据保护工作全面开展,数据中心联盟网络数据与技术协同治理委员会组织编写了《中国企业数据保护白皮书(2017 年)》。本白皮书重点分析了金融、医疗、教育、电信、电商等行业数据保护现状和问题，梳理了国内外数据保护相关法律政策，提出了企业数据保护的实践建议。

本白皮书中数据保护的定义来源于《网络安全法》对数据安全提出的完整性、保密性以及可用性三项核心要求。本白皮书可以为政府部门和企业开展数据保护相关工作提供参考。

二.研究背景

（一）数据已经逐步成为全球争夺的战略资源

近几年，随着互联网，移动互联网，云计算等产业的迅猛发展，全球数据呈指数级增长，而数据的开发利用受到各国的极大关注。大数据应用加速与经济社会各个领域深度融合，已经成为推动经济发展的新增长点。具体来看：

数据仍将保持爆发性增长。近几年来，全球数据量呈指数级增长。据国际数据公司（IDC）统计，2014 年全球数据总量为 8ZB，预计 2020 年达到 44ZB。同期，我国数据总量为 909EB，占全球数据总量的 13%。其中，媒体、互联网数据量占比为 1/3，政府部门、电信企业数据量占比为 1/3，其他的金融、教育、制造、服务业等数据量占比为 1/3。预计到 2020 年我国数据量将达到 8060EB，占全球数据总量的 18%。

我国高度重视大数据的发展。党中央提出“实施国家大数据战略”，要求加快完善数字基础设施，推进数据资源整合和开放共享，保障数据安全，加快建设数字中国，更好服务我国经济社会发展和人民生活改善。国务院印发《促进大数据发展行动纲要》，国家发展改革委、工业和信息化部等各部委纷纷出台政策措施，全面推进大数据发展，加快建设数据强国。在国家大数据战略驱动下，大数据资源建设、技术研发、创新应用等加快发展，新技术、新业态、新模式不断涌现，在稳增长、促改革、调结构、惠民生和推动政府治理能力现代化中发

挥越来越重要的作用。

数字经济已经成为中国经济增长的新动力。据中国信息通信研究院《中国数字经济发展白皮书（2017 年）》显示，2016 年中国数字经济总量达到 22.6 万亿元，同比名义增长超过 18.9%，显著高于当年 GDP 增速，占 GDP 的比重达到 30.3%，同比提升 2.8 个百分点。数字经济已成为近年来带动经济增长的新动力，2016 年中国数字经济对 GDP 的贡献已达到 69.9%。中国数字经济对 GDP 增长的贡献不断增加，接近甚至超越了某些发达国家的水平，数字经济在国民经济中的地位不断提升。

（二）数据保护是数据开发利用的重要一环

数据作为一种资源，有着重要的价值。随着数据的资源价值逐渐得到认可，不同实体对数据的需求不断增加，数据保护已在数据全产业链被提升到了前所未有的高度。在《促进大数据发展行动纲要》等一系列文件政策的推动下，我国大数据开发利用呈现出百花齐放、蓬勃发展之势。但总体来看，数据保护问题仍然是未来很长一段时间需要面临的重要问题。主要原因有以下几个方面：

行业应用的增长猛增，带来了数据保护的新期待。我国潜在的数据资源非常丰富，并在不断“挖掘”、“开采”中。整体来看，数据已在以金融、医疗、教育、电信、交通等为代表的各个行业得到利用。但是，虽然当前的数据存储和挖掘技术已经成熟，但“数据孤岛”的大量存在，制约了数据的流通和变现。还需各个行业、部门不断打破

信息壁垒，提高数据使用效率。可以预想到，随着各个行业数据开放程度的不断提高，数据应用业务会呈现“井喷式”增长，而各行业对数据保护的期待也将不断提高。

信息技术的快速演进，带来了数据保护的新挑战。在云计算、大数据、移动互联网和人工智能等技术的推动下，信息系统的软硬件架构不断发展变革，在提升数据采集、存储和分析能力的同时，也会在软硬件方面引入未知的漏洞隐患。而现有的安全防护技术还停留在“对症下药”的阶段，在抵御未知漏洞时显得束手无策。例如，大数据技术采用底层复杂、开放的分布式存储和计算架构，使得大数据环境下安全边界变得模糊，给传统安全防护技术带来了全新的挑战。

黑灰产的迅猛发展，带来了数据保护的新需求。据媒体报道显示，目前中国网络黑灰产业的年产值已达千亿人民币，而网络安全产业规模不到300亿人民币。黑灰产业从业者利用大数据的能力甚至超过一些知名互联网企业，他们能够非常精准地获取数据，进行精确诈骗。另据国家互联网应急中心监测，今年上半年我国境内被植入木马的网站达到1.8万个，收录各类高危漏洞2412个，还出现了勒索病毒和木马大面积爆发等突发事件，造成了非常恶劣的影响。

（三）加强数据安全立法已成为国际趋势

数据保护是网络安全的重中之重，对于维护国家安全、经济安全，保护公民合法权益，促进数据利用至关重要，国际社会对此普遍关注，数据保护问题也成为近年来各个国家的立法重心。

围绕数据保护立法，各国立法中要求企业建立健全以下的制度：数据的分类，备份、加密，数据防窃取或者篡改；数据留存、公民个人信息保护等，这些本属于数据安全立法领域的传统议题，但在新的网络安全形势下，也不断延伸出新的议题，如数据泄露、跨境数据流动等。

众多国家已经建立了数据泄露通知制度和跨境数据流动制度，以完善本国的数据安全保护工作。**数据泄露通知制度**（Data Breach Notification）是指在数据丢失、被窃，或者遭遇未经授权的接入，致使敏感的、可识别个人身份的数据信息的机密状态、完整状态存在受损可能，一旦发生上述情形，相关责任主体需在一定时限内向受损主体或有关执法主体进行通告。数据泄露通知制度为美国隐私保护立法首创，但近两年来被各国广泛采纳。欧盟 2011 年修订《电子通信行业隐私保护指令》时也引入了该项制度。**跨境数据流通制度**是指，一国从维护本国用户隐私以及国家网络安全的角度，对个人数据，以及涉及到国家安全的数据跨境流动做出限制性规定。例如，在澳大利亚，政府有权对一些重要数据进行审查，否则不得转移。数据被标识为“AUSTEO”和“AGAO”，确保被审查和批准后，才能向受信任源外的人开放，并须以权威机构所认定的方式转移。

我国也高度重视数据保护的立法工作。《网络安全法》已于 2017 年 6 月 1 日正式实施，立法明确了数据保护有关管理规范。从国家层面来看，《网络安全法》是我国第一部全面规范网络空间安全管理的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、

化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。**从社会层面来看**，《网络安全法》对网络运营者数据保护的义务性要求进行了进一步明确，对企业的发展运行也提出了更高要求，将促进整个社会数据的开发利用朝着健康有序的方向发展。**从个人角度来讲**，《网络安全法》设专章规定了“网络信息安全”，针对用户个人信息保护提出了大量具体要求，将个人信息保护明确纳入网络运营者实施网络安全风险管理的必要内容，具有重要影响。

三.行业数据保护现状及问题分析

随着信息技术迅速发展和迭代，互联网已经不再是单纯狭义的互联网概念，而是将互联网，大数据，云计算，包括物联网这些新兴的信息技术全部打包到互联网里面，那么互联网+就是对当前诸多新兴技术的一个整合和集成。诸如金融，医疗，教育等传统行业，在与互联网行业深入融合时，可以帮助提升自己核心竞争力，加速供应链和生态链整合，并通过互联网+探索新商业模式，进而形成新的业务增长点。但是，互联网+的融合就必将涉及到各类数据的采集，存储，利用等环节，这也就将数据保护提升到了前所未有的高度。

本节将结合数据中心联盟联合相关公司的部分调研数据，针对金融，医疗，教育，电信等行业，详细分析该行业信息化及数据保护的发展现状，并重点分析目前这些行业数据保护工作中出现的一些核心问题。

（一）金融行业数据保护现状及问题分析

当前，我国金融业信息技术在充分融合金融业务发展需要和信息化建设实际的情况下，在金融信息基础设施、宏观调控信息化和监管科技应用、网络安全保障及信息技术治理体系等方面取得了丰硕成果。随着金融普惠发展的创新活力日益增强，金融行业数据极大丰富，在此背景下，我国在金融行业数据安全保障能力、金融信息技术治理体系方面已经取得了很大进展。

随着金融行业的高速发展，金融体制改革和金融业务发展对行业数据保护提出了新需求，金融风险和网络安全形势也为行业数据保护带来了新的挑战。金融信息系统业务覆盖率和复杂度持续提升，要求金融行业在总结数据保护已经取得的成果之上，充分认清面临形势和挑战，攻坚克难，切实抓住金融与信息技术融合加速创新发展的机遇。

为进一步梳理金融行业数据保护现状，便于金融企业更加客观的认清金融行业数据保护现状及面临挑战，我们依托第三方媒体机构，对 100 余家金融机构进行了问卷调查，包括大型国有银行、商业银行、证券公司、期货公司、基金公司等。现将调研情况总结如下：

1．数据保护治理能力显著提高

行业数据保护顶层设计持续加强。当前，我国金融行业能够落实国家数据保护相关保护制度，持续强化金融数据安全风险预警和数据共享，加强金融业与技术支撑单位的协作，有效提升了金融数据保护

的联防联控水平。

数据保护管理水平持续增强。我国建立了较为完善的信息安全管理组织和制度体系，为行业数据保护打下坚实基础。银行、证券等级保护系列标准的制定推动了数据保护测评工作的顺利开展；信息安全检查工作促进了信息技术风险管理水平提升；重要时期网络安全保障工作确保信息系统安全、稳定运行；互联网网站安全专项整治工作提高了互联网网站数据安全防护能力。

数据保护监管体系和协调机制进一步优化。我国金融机构及监管部门均已设立专门信息技术监管和服务部门，组织架构进一步完善。以金融标准化技术委员会为例，其组织架构、工作制度和协调机制持续完善

数据保护技术治理和资源配置持续优化。各主要机构逐步建立了与自身运营模式相适应、职责清晰的信息技术治理架构，行业数据保护成为其重要一环。各金融机构数据保护履职力度逐步加大，队伍建设不断加强

2．数据保护技术治理体系不断优化

金融标准化战略深入实施。截至“十二五”期末，我国共制定金融标准 179 项，其中，国家标准 53 项，行业标准 126 项，覆盖领域持续扩大，标准内容涵盖行业数据保护主要内容，并由信息技术规范向业务和管理领域拓展。我国全面推进金融机构标准化工作，建立了金融标准认证机制，开展了标准实施检查评估，夯实了金融标准化

工作基础，为金融行业数据保护营造了优异的环境。

数据保护技术能力不断提升。目前我国金融信息系统主要采用物理隔离、逻辑隔离等技术手段加强行业数据安全防护，实施电子认证、数据加密等技术，积极推进安全可控技术应用，成功实施符合国家要求的密码算法应用试点示范工程，基本建成覆盖物理、网络、系统、应用、数据和终端等领域的端到端的网络安全技术防护体系，金融业数据安全保障能力显著增强。

3．数据保护存在突出短板问题

尽管我国金融行业数据保护已经取得极大进步，但仍然存在突出短板问题。当前金融数据共享和开发利用水平不高，监管科技水平不能满足金融治理体系和治理能力现代化的需求，数据保护技术相对落后；传统金融机构在新技术应用和分布式架构转型方面进展较慢，行业数据保护相关举措未能有效跟进；金融业标准化协调推进机制有待进一步完善，相关数字资产界定及相关保护举措尚未形成标准；同时一些机构和部门数据保护意识淡薄，数据保护管理水平不高，行业数据安全面临严峻挑战；金融信息技术治理水平及相应的数据保护举措不能有效适应现代金融业发展的需要。

敏感信息保护还需加强。防范信息泄露风险是数据保护工作的重中之重。近年来，徐玉玉等多起网络电信诈骗事件，再次引发了社会各界对个人数据安全的关注。金融行业机构需着重从源头加强数据信息保护。随着交易的爆炸式增长，金融机构要对客户线上线下交易等

各方面信息进行广泛、全方位地搜集，通过相关数据模型，科学分析并保存。对这些海量信息管理不当，会造成客户个人隐私信息的“泄露、丢失”。很多金融机构没有在“采、传、存、密、用、毁”等各环节建立起数据保护有效机制，使得数据泄露风险日益加剧。一方面建立系统的数据保护机制、预警机制、应急机制，时刻做好信息安全防范工作；另一方面在数据信息的应用中，严格遵守国家政策、法规，避免滥用信息，侵害消费者权益。

企业数据泄露问题突出。企业数据泄露主要由外部黑客攻击和内部人员泄露两部分原因造成。据调查统计，外部黑客攻击互联网金融平台的目的主要为窃取数据，占比高达 48%，其次为敲诈勒索和商业竞争。通过攻陷大批互联网金融平台，引起系统瘫痪。据 IDC 调查报告显示，来自于企业内部的数据泄露风险及网络安全威胁超过 85%，其危害程度远远超过黑客攻击所造成的损失，而这些威胁绝大部分是企业内部各种非法和违规的操作行为所造成的。

金融行业由于业务的特殊性，与一般行业间也存在着一定的区别，传统的安全防护机制下造成数据保护风险的原因主要以下几个方面：

（1）数据的分散存储；

（2）数据加密技术不成熟；

（3）缺乏独立的工作环境；

（4）人员安全意识水平参差不齐。

（二）医疗行业数据保护现状及问题分析

随着国家卫计委 “46312”工程的开展，国家医疗信息化的政策也越来越完善，分级诊疗、医联体、异地就医、三医联动等一系列新型医疗服务模式正在大力展开，个人健康档案、患者信息、临床数据、执业医师信息等各种医疗数据都流通在这些平台及业务系统上，此类数据行业价值巨大，如何保护这些重要数据显得尤为重要。

1．医疗数据“物理隔离”仍将是有效的数据保护措施

据不完全统计，我国医疗机构中可明确管理的数据资产数量只占到总信息资产的 70%。这就意味着，在医疗机构内部，有一部分“数据”存在于“非信息系统上”，或者是，这部分数据是在“物理隔离”的场景下存放的。究其原因，一部分“数据”涉及国家重要人员的病例信息，属于国家机密；另一部分“数据”来自于艾滋病、肝炎等患者的个人信息，这类隐私数据往往不宜“公开”。由于医疗从业者对信息系统存在“不信任”情绪，而采取的数据保护措施就是“纸质病例存储”或“信息系统物理隔离”。现阶段，在无法百分百确保信息安全的状态下，这种数据保护的措施仍将被利用下去。

2．数字化医疗带来了对数据保护的新要求

在移动互联网、云计算、大数据、人工智能等技术的驱动下，医疗机构正在向数字化医疗模式转型。在提升工作效率、改善生产模式的同时，也不可伴随着新的问题和挑战。2017 年，国内医院大力推

广“互联网+医疗”服务，已有千余家医院自主研发或者委托第三方开发的移动应用程序，各类网上挂号系统、远程诊疗系统如雨后春笋般出现，这些系统往往需要采集患者的姓名、身份证号、联系方式等个人数据，但是这些“第三方入口”的安全性有待商榷，一旦数据被别有用心人员窃取，将可能用于非法用途，造成的损失不可估量。

3．医疗从业人员的信息安全意识仍要继续提高

信息安全意识不足是各行各业普遍存在的问题，医疗行业也不例外，由于工作人员安全意识不足造成数据泄露的案例也层出不穷。即使经过专业培养的员工，由于粗心大意或工作失误带来的数据泄漏风险也不可能完全避免。目前来看，医疗行业从业人员，由于工作压力大，缺乏专业教育培训等因素，在从业过程中，对信息安全问题的重视程度仍然有待提高。

4．充足的信息安全预算将是开展数据保护的必要前提

据调查显示，我国医疗机构中，约 54%的被调查人员认为现有的信息安全预算不足，希望增加预算。现有的信息安全预算往往是根据医疗信息化部门对本机构的信息系统风险的预判而设置的。信息安全预算的不足，确实能节省整个医疗信息化系统的建设开支，但是，从长远来看，医疗机构数据泄漏的风险将会不断加大，而数据泄露的损失将远大于前期用于信息安全建设的投入。因此，充足的信息安全预算，将是有效开展数据保护工作的必要前提。

（三）教育行业数据保护现状及挑战分析

“信息技术对教育发展具有革命性影响”，教育信息化全面推动教育现代化是信息时代我国实现教育改革和发展的重要战略决策。过去几年，全球信息技术发展迅速并深刻影响教育教学。高速互联网、移动通讯、云计算、大数据和智能产品等新一代信息技术在全球教育领域产生深刻影响。具体体现在以下几个方面：一是学校网络教学环境大幅改善，全国中小学校互联网接入率已达 87%，多媒体教室普及率达 80%;二是优质数字教育资源日益丰富，信息化教学日渐普及，全国 6000 万名师生已通过“网络学习空间”探索网络条件下的新型教学、学习与教研模式;三是教育资源公共服务平台服务水平日渐提高，资源服务体系已见雏形;教育管理公共服务平台基本建成，覆盖全国学生、教职工、中小学校舍等信息的基础数据库，并在应用中取得显著成效;四是 MOOCs、翻转课堂、创客教育和 STEAM 教育等信息技术支持的新兴教育、教学模式蓬勃发展。据统计，2015 年我国互联网教育全产业规模预计将达 1192 亿元，并在未来两年内保持 21%的增速；用户规模达到 1.10 亿人，占网民数量的 16%左右，其中手机端在线教育用户规模为 5303 万人。目前，“互联网+”教育领域囊括了 K12（幼儿园到 12 年级）、职场教育、兴趣教育、技能培训等领域。

但是目前教育行业很多学校和机构的数据保护理念，制度及手段仍未适应新兴信息技术的发展，只管建设不顾安全、只管硬件忽视

软件、只管数据采集不顾数据维护的粗放式管理模式比较普遍，学校网络安全事件，泄露学生隐私，学校数据库被攻击等事件时有发生。如河海大学、广西民族大学、西安音乐学院等高校近几年在进行国家奖学金候选人或获得者名单公示时，均披露了学生完整的公民身份证号码。2016 年，某省某准大学生因考生学籍信息非法泄露而被骗走全部学费以致昏厥猝死。

2017 年教育部已经联合公安部等相关主管部门出台了相关制度和要求，但总的来看，教育行业的数据保护虽已取得部分进展，但仍存在数据标准和评测机制尚未形成，相关安全制度和人员培养机制缺乏等问题，具体体现在以下两个方面：

1．数据保护制度逐步建立，标准和评测机制尚未形成

教育信息化是国家信息化重要组成部分，教育行业网络与信息安全工作关系着教育信息化的稳步推进和教育事业的改革发展。为加快建立健全教育行业网络与信息安全保障体系，提高防护能力和水平，保障教育事业健康有序发展，教育部联合相关部委陆续发布了《教育部关于加强教育行业网络与信息安全工作的指导意见》,《教育行业信息系统安全等级保护定级工作指南》,《教育部公安部关于全面推进教育行业信息安全等级保护工作的通知》等一些列措施，对教育行业网络与信息安全提出了相应的要求。

但是，综合教育行业网络与信息安全的特点，信息安全等级保护有关的定级指南、基本要求、测评规范、综合评估体系等行业标准规

范和评测规范仍然缺乏，亟需完善相关标准和评估体系，对教育行业网络与信息安全实现科学化、规范化和制度化管理。

2．信息安全得到高度重视，安全制度和人才建设滞后

经 2016 年、2017 年一些列教育领域造成严重后果的数据泄露事件发生之后，各大学校和教育机构已经将防范信息安全事件发生作为重要工作。

但是大部分教育机构信息安全事件经过事后调查发现，主要的数据泄露不是来自于互联网攻破，而绝大多数皆因内部监控疏漏或内部人员有意或无意为之，如内部人员故意泄露、合作机构拥有信息系统权限、计算机遗失导致的“被动”泄密。造成这一现象主要原因是安全人才队伍的缺乏和数据保护的理念落后。

在数据保护的理念方面，许多教育机构对数据泄露问题理解不深、准备不足，在内控上缺乏投入，虽然采取封掉 USB 接口、限制上网、制定信息访问权限等诸多手段，但依然有大量的教育敏感数据、用户信息通过电子邮件、即时通讯工具、U 盘等泄密到教育机构外部。

在制度建设方面，各单位亟需结合自身实际，制定网络与信息安全总体规划，加强安全管理策略研究，建立并完善本单位加强网络与信息安全管理所需的各项规章制度，重点包括人员安全管理、计算机软硬件管理、信息系统建设与运维管理、门户网站管理（包括内设机构建设的各类网站）、邮件服务系统管理、数据安全及使用管理等制度，并在实际工作中予以落实。

在安全人才方面，各单位普遍缺乏具有网络和信息系统管理经验和专业技能的人员，更没有网络与信息安全管理专职队伍和技术支撑专业队伍和相关的网络与信息安全的培训规划。

（四）电信行业数据保护现状分析

1．我国电信行业数据保护立法体系初步建立

我国于 2011 年和 2013 年分别制定了《规范互联网信息服务市场秩序若干规定》及《电信和互联网用户个人信息保护规定》，目前正在制定《电信和互联网网络数据管理暂行办法》，用户个人信息保护进入监管落实的关键期。

2．用户信息保护得到高度重视，数据泄露风险仍然存在

当前我国多数电信运营企业能够按照国家相关法律法规要求，制定客户信息保护制度，但在风险检查中发现，部分一线公司对相关制度落实不到位，告知统一落实不到位、代理商监管存在漏洞、内部信息泄露等现象仍有发生。虚拟运营商同时也存在重视程度不高的情况，重经营轻服务，忽视用户信息保护工作，缺乏专门的内部规章制度，且法律法规落实不够到位，一些虚商的服务协议未包括用户信息条款，服务过程未满足用户的知情权等，对用户的信息安全构成了威胁。

3．数据安全标准有待健全，风险管控力度还需加强

电信大数据涉及用户个人隐私，在用户数据安全和信息保护方面

要求严格。如何在数据交易过程中，有效规避数据安全风险，切实做好数据安全管理和保障，是电信大数据应用发展必须面对的重大挑战。当前，大数据安全领域的相关标准仍处于探索期，涉及电信大数据应用的安全规范更是存在较多空白。在缺乏行业统一安全标准和管理规范的情况下，单纯依靠企业自身管控，会带来较大的安全管控风险。

4．数据管理能力有待提升，软件开发能力存在短板

电信企业传统的数据系统是“烟囱”式建设，数据分散在各个系统中，缺乏统一的数据存储管理标准，“三域”数据整合仍处于建设阶段，不同领域的数据壁垒仍较为明显，而且系统改造难度大，短期内难以改变。同时，现有的数据采集和应用分析能力是基于传统结构化数据形成的，难以满足大数据业务的海量数据存储和非结构化多样性数据计算要求，数据需求响应速度慢，个性化分析能力不足。此外，传统电信业务的多层级运营架构，难以适应大数据业务的灵活运营特点和快速创新趋势。对我国电信企业而言，发展大数据业务在组织架构、人才储备和运营流程等方面均面临较大的转型调整压力。

（五）电商行业数据保护现状及挑战分析

1．电商方面的专门立法加速，数据保护成为关注焦点

据《2017 年（上）中国电子商务用户体验与投诉监测报告》显示，2017 年上半年中国网购用户达到了 5.16 亿人，较 2016 上半年的 4.8 亿人，同比增长了 7.5%。预计 2017 年中国网络购物用户规模将

达到 5.4 亿人。电子商务的蓬勃发展，催生了对专门立法的客观需求。实际上，早在 2013 年，中国全国人大常委会就已经启动了《电子商务法》的立法进程。目前，《电子商务法》已结束二审，预示着这部法律即将出台。在这部即将出台的法律中，对网络交易中的消费者数据保护问题，给予了高度关注，特别是《电子商务法》草案中“关于电子商务交易保障”的第四章，专门规定了电子商务数据信息的相关问题，并对消费者数据保护的法律制度构架、个人信息的范围、收集原则以及个人信息的处理和利用等问题进行了明确。

2．电商行业生态链不断延展，催生了对数据保护更高要求

电商行业的庞大用户群体，为数据的搜集和汇聚提供了先天的基础。现有的电子商务活动中已经涵盖了用户的消费、生活、出行、物流等多方面的数据，电商平台以此为基础，不断拓展自己的业务板块。特别是在大数据、人工智能以及移动支付技术的推动下，我国的电子商务平台业态百花齐放。从纵向来看，电商平台已经开始进军无人零售、生鲜电商、社交电商、精品电商等新兴热门行业；从横向来看，电商平台已衍生出信贷、保险、理财、征信、通信等增值服务板块，并取得了良好效果。而这些业务和应用的使用，必然会带来新的安全风险，对数据保护的要求也将更高。

3．黑灰产攻势不断加强，电商平台安全投入持续加大

近年来，电子商务异军突起，势不可当，与此同时，非法盗取、

泄露、买卖用户数据、网络诈骗等问题随之彰显，甚至形成了地下产业链。在利益的驱动下，电商平台数据成为黑灰产从业人员竞相争夺的“蛋糕”。在变幻莫测的攻击手法面前，电商平台也不断加大安全投入，积极采取安全保护措施。据某电商安全负责人介绍，他们在数据保护方面投入了大量人力、物力，比如：对于用户数据进行了严格的加密，对数据存储权限进行严格限制，在传输层面也实现了加密传输，全方位保护数据安全。

四．企业数据保护存在问题和挑战分析

综上可以看出，尽管企业已采用各种手段进行数据保护，但数据泄露的事件仍然经常发生，甚至造成了非常严重的社会影响。数据泄露事件在一些制度、技术都较为健全的企业中也无法避免。根据调查结果及上述分析，目前在我国企业中数据安全方面主要存在有以下问题和挑战：

1．制度建设缺失

虽然我国有众多的数据保护规范性文件，但是在现行的法律规范中，立法主体多、体系繁杂、没有统筹规划的问题突出，不能够适应新形势下的数据保护保护工作。主要存在的问题有：

1）法规建设滞后，没有总体的规划；

2）规范不能互通和协调，尤其不能注重结合行业特点，可执行性不高；

3）一部分规范已经不能够应对新型的数据保护威胁；

4）部分规范不能够得到落实。

2．技术手段落后

纵观国际安全形势，我国数据安全使用技术手段仍然比较落后。多数的企业只使用了基本的数据安全手段。

（1）终端管控技术仍然是主流手段

终端是数据存储和使用的主要位置，终端具有分布散，数据类型多的特点，并且终端上的数据多数为非结构化数据，还存在有文档格式处理复杂的问题。因此，多数企业对终端的数据安全主要以管控为主。通过管控技术，对终端的数据外发通道进行限制，比如关闭蓝牙、USB 存储等数据传输通道，对终端上安装的软件进行限制，对终端对外发起的连接进行监控和阻止等方式和手段。终端管控有效的控制了终端对外的数据传输，但同时也降低了终端的数据交互能力，降低了工作的效率。并且，由于缺乏对内容的分析手段，单纯的使用终端管控手段仍然无法有效的了解终端上的数据内容的分布情况和控制数据内容的传输。

（2）加解密技术在艰难中前行

目前，加解密技术在数据安全中得到了广泛的应用，包括终端的存储加解密，网络传输加密、应用、数据库加密等多种位置、通道都可以使用加解密技术。加解密技术可以有效的防止数据被窃取之后的使用问题。比如终端的硬盘透明加解密可以保护在电脑丢失后，即使

将硬盘挂接到其他机器上也不能获取其中的内容。传输的加解密可以防止中途的窃听，窃取。数据库加解密可以防止拖库后数据被使用的情况。但加解密方式在保证安全性的同时，也带来了应用系统处理复杂，数据交换困难，管理维护复杂等相关的问题，在实际使用中总是会造成对工作流程的较大困扰。

（3）数据安全缺乏管理手段

和其他的技术型安全防护（如杀毒、DDoS 防护）等安全方向不同，数据安全综合了管理、流程、技术的安全防护手段。在数据安全体系中，技术手段只是实现的方式，更多的需要管理流程、组织架构的介入，在多数企业中发现，很多企业都没有清晰的定义或者了解自己企业最重要的数据是什么，哪些数据是需要保护的，这些数据存于哪些人员或者应用系统中。在这种情况下，没有一个整体的管理流程、人员组织结构定义来支持数据安全，光凭借技术手段很难实现有效的数据安全管理。

3．安全意识薄弱

在多数的企业中，业务人员缺乏数据安全意识，企业数据随意分布。比如缺乏对 U 盘使用的管控，以及弱口令的使用，带来了各种社工、撞库等入侵风险。在实际生产中，更多的数据泄露通道常见于网盘的上传和邮件外发中，这两个通道是最为便捷的数据外发方式和手段。

当前，企业在安全方面的投入主要用于防护外部攻击手段，如防

火墙、IPS、IDS、WAF 等技术。从数据保护的角度来看，阻止外部人员入侵是基础条件，但这些手段很难对内部人员主动或无意的泄密进行防护。另外，针对当前流行的 APT 攻击手段，这些针对外部的安全防护手段也很难起到实际的作用。

4．安全人才紧缺

和其他的运维、开发、技术支撑等岗位相比，安全管理人员的要求会更高，一个合格的安全人员必须同时具有业务理解能力、工程管理能力和全面的技术能力才能真正的胜任企业的安全防护责任。而这方面的人员由于其需要跨专业、跨能力范围，因此能满足要求的人员整体较少，安全人才在全国范围甚至全球范围都是紧缺资源。安全人才的紧缺也是造成很多企业在安全事件前措手无策的原因之一。

五．企业数据保护建议

我国立法中对企业的数据保护义务存在与以下两个方面：一是履行数据安全保护义务，防止网络数据泄漏或者被窃取、篡改，二是承担用户个人信息保护责任，防止侵害公民对其个人信息享有的权益。而落实好企业的数据安全保护义务，是实现企业数据保护工作的重中之重，本节对企业如何开展数据保护工作提出了相应建议。

数据保护并不单是制定了法律和行业指导规定就可以结束的，最终还是需要落实到各个具体的企业中去，每个企业都将自身所拥有的数据进行有效的保护以后才能形成全社会的合力，全面实现数据安全

防护。

数据保护，分为前期规划、建设、实施操作三大阶段。

（1）规划阶段：根据法律法规相关要求，结合企业自身情况，制定企业的数据保护规划的方针和策略。

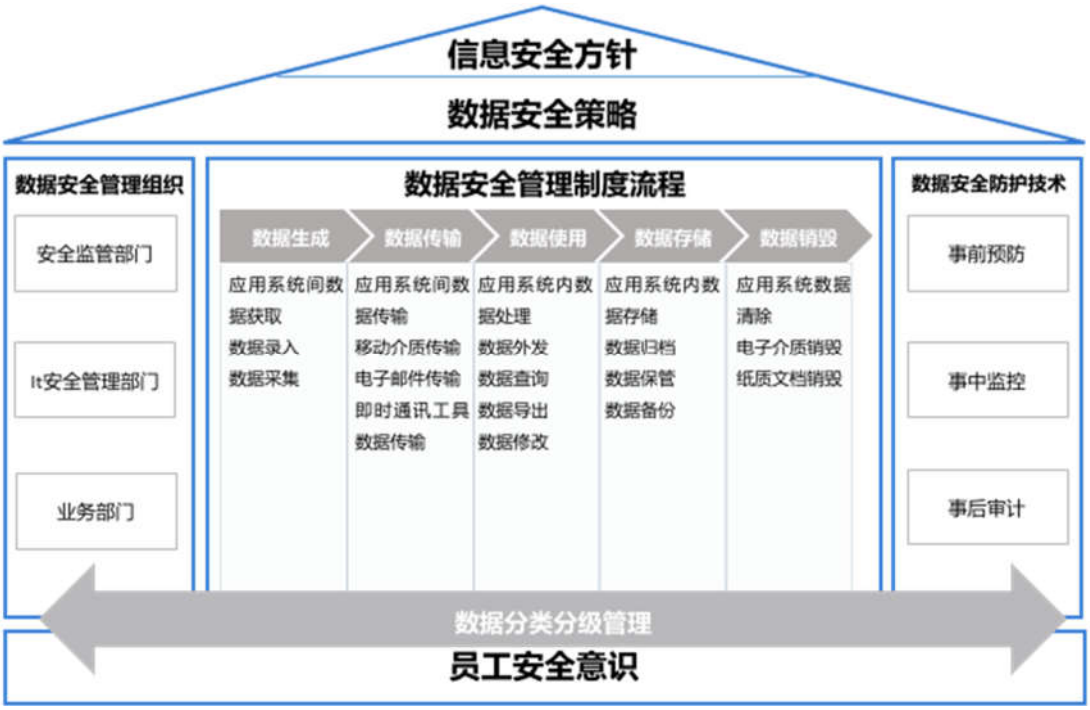
（2）建设阶段：按照规划的方针和策略，组织适当的组织架构管理，制定相关的管理流程制度，并选择适合于本企业实际情况的技术手段加以实现。

（3）运行阶段：数据安全建设并不是一蹴而就的，需要在实际运行过程中进行不断的调整，最终实现数据安全的全面管控。

数据保护是一个长期的过程，在这个过程中，企业应当注重建设自身的人才队伍，培养自身的数据安全团队，才能不断提高企业的数据安全防护水平。

（一）规划阶段

企业在考虑进行数据安全体系化建设的时候，可以首先根据国家法律法规，结合本企业的实际情况，制定企业的信息安全方针，在方针的指引下制定相应的企业数据安全策略。根据企业数据安全策略，建立相应的企业数据安全管理组织，按照数据生命周期制定数据安全管理流程制度，最后通过相应的数据安全防护技术实现对数据安全策略的贯彻。



在企业数据安全的规划阶段，主要需要从以下几个方面进行考虑：

1. 企业合规计划

《网络安全法》现已发布，作为我国首部网络安全领域基本法，在信息化领域具有里程碑意义。《网络安全法》在国家关键信息基础设施运行安全、网络信息安全、监测预警与应急处置等内容进行详细规定。《网络安全法》将个人信息保护予以明确，同时就“防止网络数据泄露或者被窃取、篡改”，明确要求“采取数据分类、重要数据备份和加密等措施”。

企业应根据国家法律要求和自身所在的行业规定、指导等要求，结合本企业具体情况有针对性的制定相关标准。比如针对网络安全法中规定的个人隐私数据类型在本企业中存在的位置、使用情况等进行

分析和评估，另外一些行业性规定比如证券期货行业的数据分类分级相关标准、规范、指引，以及个人信息保护的相关规定，对于证券行业企业就需要进行认真的分析并制定本企业的企业数据安全策略。

2. 企业数据安全相关制度建设

- 多维度管理，“三管”齐下

多维度数据安全管理工作，促进数据安全的落地实施。“三管”即从以下三个方面进行数据安全管理：

组织与人员：梳理信息安全职能职责，岗位要求明确；人员配备人数合理，人员具备岗位需求能力。

制度与流程：在数据安全管理方面建章立制，并有相应流程支撑。

技术与工具：具备适当的工具、产品等技术手段支撑数据安全管理。

- 数据分级分类，抓住重点保护对象

通过对数据分级分类的方式，筛选出重点保护对象，进而对数据进行敏感性标识。根据数据的敏感性，采取不同的保护措施。

- 识别数据场景，管理数据生命周期

识别数据的使用场景，并梳理数据的生命周期。数据生命周期包括：数据产生、数据采集、数据传输、数据存储、数据使用、数据销毁。控制数据生命周期每个节点的安全性。

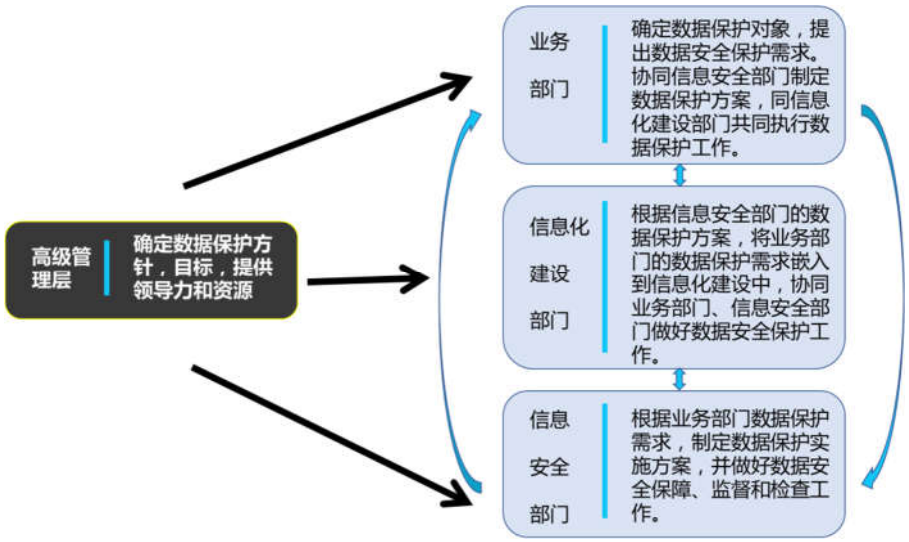
- 关注数据合规要求，保证基本底线

结合法律法规要求、相关方要求、合同要求，保证数据合规性底

线。

相关方可以是监管机构、甲方、乙方、合作伙伴等。

3. 企业数据安全组织架构



数据保护的组织层面，需要有高级管理层、业务部门、信息化建设部门、信息安全部门共同参与。

高级管理层确定数据保护的方针、目标、提供数据保护工作的领导力和资源，并总体协调业务部门、信息化建设部门、信息安全部门。

业务部门确定数据保护对象，提出数据保护需求。协同信息信息安全部门制定数据保护方案，同信息化建设部门共同执行数据保护工作。

信息化建设部门，根据信息安全部门的数据保护方案，将业务部门的数据保护需求嵌入到信息化建设中，协同业务部门、信息安全部门做好数据安全保护工作。

信息安全部门，根据业务部门数据保护要求，制定数据保护实施

方案，并做好数据安全保障、监督和检查工作。

在大型企业中，建议增加首席数据官或者数据安全官的人员岗位，对企业的整体数据治理以及数据安全负责。

4. 企业数据安全防护技术选择

围绕数据安全生命周期，包括数据的生成、传输、使用、存储、销毁的全生命周期，从 IT 技术上有各种各样的相关产品围绕着数据的安全防护。

总结起来，数据安全防护主要有以下技术手段：

1、身份认证：身份认证技术是在计算机网络中确认操作者身份的过程而产生的有效解决方法。身份认证方法包括：静态密码、智能卡、短信密码、动态口令牌、密钥、数字签名、生物识别技术等。

2、访问控制技术：指防止对任何资源进行未授权的访问，从而使计算机系统在合法的范围内使用。意指用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用的一种技术。

3、加密技术：传输加密和存储加密。传输加密是指在传输过程中通过加密手段对流动中的数据进行转换，从而确保数据在传输过程中的不可识别性，预防出现中间人劫持导致数据外泄。存储加密的应用包括数据级加密、文档加密、磁盘加密、透明加密等。通常，在加密技术中往往也会同时结合访问控制技术。

4、内容分析技术：对存储中的数据、使用中的数据和传输中的

数据的内容进行即时的识别、分析和处置。

5、审计技术：将不规范操作或非法入侵的痕迹通过技术手段进行留存，以供日后进行复查及追溯。常见的审计技术包括日志审计、数据库审计等。

（二）建设阶段

建设阶段主要是将企业的整体数据安全规划进行实施。在这个过程中，通过设置设定适当的人员组织架构，制定相关数据保护制度和行为管理规范，并通过相关数据保护技术进行部署，贯彻和完善企业的整体数据安全规划。

在建设阶段，数据保护技术可以按照以下步骤进行实施规划：

第一步是“精准打击，明确需要保护的对象”。“无差别防护等于没有防护”，所以数据保护要具有针对性。对大部分企业来说，首要需求都是合规性，企业必须符合《网络安全法》，还要符合各行各业自身的行业法规等。这时候就需要根据法规要求和自身情况，对企业数据安全做出相应的方式和手段。

例如，互联网企业最重要的信息是个人信息，而对传统企业最重要的信息是企业的机密信息，如知识产权、财务或者企业战略等。而对于生产型、制造型或研发型企业来说，首先要对内部数据进行分级，再对这些数据按照重要程度进行划分，根据级别打分并计算数据在发生泄漏或丢失的情况下所带来的危害性针对分值最高的数据进行优先保护，对于分值较低的数据进行次优先级的保护。

第二步“态势感知，掌握企业数据状况”。在考虑数据安全防护的时候，需要了解数据的分布、存储和传输状态，掌握相关的情报和信息，从而做出精准的决策。

首先在敏感数据定义已经明确的前提下，通过对存储的扫描，掌握敏感数据的分布情况，形成“企业的静态敏感数据分布视图”，并利用加密等保护技术确保此类敏感数据的存储安全。

其次，对于离开网络边界的数据进行详细分析，掌握谁、哪些数据、通过怎样的方式离开了企业的边界，有助于了解整个数据在企业传输的情况，进而形成“*企业的动态敏感数据流向视图*”，并依据此视图改善可能存在风险的业务流程。

最后，对用户行为进行分析。通过协议层面、网络数据包、终端信息等各种数据的采集，并将这些数据进行汇总关联后，利用人工智能进行分析和处理，还原出数据在网络的路径，形成“*以人为中心的行为分析视图*”。

这种“以人作为中心的行为分析手段”分成三个不同的层次。第一是“**异常行为检测**”，根据异常概率的统计分析，总结个体在群体中的行为异常，从而发现可疑人员行为。第二是“**精准行为预测**”，通过循环神经元网络，对用户已知的行为数据进行回溯，再对其他用户进行模型分析，预测可能发生数据泄露事件或被攻击事件。第三是“**专家统计模型**”，通过已制定的专家经验行为模式，发现企业用户行为是否可疑。这类专家模型往往比较精确，可以直接定位到发生问题的人员或电脑。

第三步“**主动防御，持续性体系建设**”。主动安全防御主要是“通过形成自适应的安全架构，实现持续分析用户和实体的行为，包括审查、规则、评分、持续画像、持续分析和验证”。主动安全防御是基于态势感知的基础之上，对每个用户进行打分，得出用户的危险分值，并对可疑的用户进行实时监测、对可疑的数据传输行为进行精准控制，防止数据泄露。

在数据保护建设阶段，因为各企业实际的环境和自身情况不同，往往需要根据自身的实际情况包括人员储备、技术储备、资金投入计划等灵活的制定本企业的数据安全规划。在这个过程中，需要着重注意以下方面的问题：

1. 安全与工作效率之间的平衡

“在确保企业日常业务正常有效地运行的前提下，最大限度保障企业的核心数据资产”是企业数据安全保护的最终目标。企业需要在“数据安全保护”与“工作效率保证”之间选取一个合适的平衡点，从而保证安全需求来源于业务并服务于业务。

2. 数据分级分类工作的持续性

有效地进行核心数据资产的保护，需要企业完成数据资产的分级分类工作。合理的数据分类定义，准确的类别等级设定以及明确类别等级相对应的操作贯穿在整个企业数据资产保护过程中。随着企业业务不断发展以及公司规模、组织架构发生变化，上述的数据分类分级动作也应持续运行。

3. 各部门之间的紧密配合

过往的事实证明，数据资产保护仅由单个部门发起、规划、建设及维护是失败的。其分布性决定了数据保护需要企业各部门的紧密配合。在进行数据保护规划设计时，应了解并掌握业务部门的实际需求，结合内审部门的数据保护规范，并通过技术部门选择的保护技术落地。通过部门协作，细化数据保护策略，提高效率并减少处理工作量。

4. 全员数据安全教育

根据以往安全事件统计报告可以发现这些安全事件中，绝大多数的安全事件都是由企业员工、外包人员以及其他有权访问机密信息的工作人员造成的。同时，大多数事件是由于员工无心之失或政策理解错误引发的。为了减少这种内部人员所带来的威胁，企业必须对员工进行安全培训和意识教育来改变其行为。通过制定员工教育的长期计划和目标，再将长期计划分解成具体、可执行的短期计划。将安全知识转换成为员工能懂的语言，并选择不易引起员工反感的宣传教育形式以拉近信息安全宣教工作本身与员工之间的距离。

（三）运行阶段

在实现了数据保护建设后，即进入数据保护的运行阶段。在这个阶段，监管机构以及内部和外部的审计人员通常会查找企业内主动、持续防范风险的证据。为了实现合规目标，在该阶段企业必须权衡数据保护策略是否随时间的推移而行之有效，以便了解潜在的违规情况、揭示明显的数据风险趋势并修补不完善的业务流程。

在这个阶段，数据保护的执行报告是满足合规要求并验证风险随

时间的推移而不断降低的关键步骤。高管理人员希望主要了解下列内容:

•当前已量化的风险。这使高层管理人员可以深入了解数据风险，以便将其置于其他企业风险领域的环境中加以考虑。

•基于企业领域的风险。对最大的风险领域了如指掌之后，企业便可将目标锁定于必须遵从要求的操作所处的特定领域。

•潜在的法规风险。由于企业承担的责任与国际、国内以及行业的数据法规相关联，这就需要明确这些责任。

•风险随时间的推移而不断降低。这项分析结果可能是最重要的，因为它证明了为减少法律责任而主动采取了相应措施。

上述的三个数据保护阶段是从数据规划阶段开始，最后进入运行阶段，这里并不存在所谓的数据保护终止阶段，三个阶段周而复始，形成数据保护的持续性优化改进闭环，是数据防护能力不断提升的“保障”。

附件：国内外法律法规现状

（一）美国数据保护法律制度

近年来，美国一直是全球数据隐私和安全监管领域的引领者。目前为止，美国并没有统一的联邦数据保护立法，在各领域采取了分散式立法的模式，在电信、金融、健康、教育、儿童在线隐私等等领域都有专门的立法，构成了一整套的联邦数据保护相关法律体系来管理数据保护的各环节。

1．数据保护立法概况

美国在数据保护方面首先是区分政府部门与私营领域分别进行立法。比如美国个人信息保护最主要的立法 1974 年《隐私法》（The Privacy Act of 1974）仅仅适用于政府部门，不适用于私营部门。《隐私法》适用范围仅为联邦政府部级、委员会以上级别的机构收集处理个人信息，保护客体为政府机关在履行行政职务过程中掌握的个人信息记录。主要对个人信息的收集、持有、存储以及传输的相关原则和具体程序做了详细规定。

其次是针对私营领域，采取了分行业、分领域立法的模式。在电信、金融、健康、教育、儿童在线隐私等等领域都有专门的立法。比如针对金融领域的《公平信用报告法》（The Fair Credit Reporting Act）为规范私营部门使用个人信息的第一部联邦法律。要求信用报告机构遵循合理程序来保证与提高个人信息的准确性、公平性、隐私性，主

要调整了征信和授信业务链中的个人信息利用与保护问题。此外美国各领域针对数据隐私和安全要求的重要立法还有《金融服务现代化法》（The Gramm-Leach-Bliley Act，GLBA）、1996 年《健康保险便利及责任法》（The Health Insurance Portability and Accountability Act of 1996）、《FTC 法》第五条（Section 5 of the Federal Trade Commission (FTC) Act）、《电子通信隐私法》（The Electronic Communications Privacy Act ("ECPA") ）、“儿童在线隐私保护法”（The Children's Online Privacy Protection Act ，“COPPA”）等。

再者，联邦和各个州都有分别的立法。州层面的立法不仅仅局限于在联邦法的立法内容体系下，甚至有些州立法规定的更为具体与详细，如果不能了解相关的州立法，无法对美国的隐私保护状况进行正确的评估。

除了相关的法律法规和司法裁判之外，美国的隐私和安全格局还有自律守则，政策和契约义务。企业和其他组织的信息隐私实践不仅受到适用法律规则的驱使，而且受到民事诉讼（特别是集体诉讼）、监管压力以及与潜在数据隐私和安全违规相关的声誉风险的驱动。

2．数据保护的原则

美国国务卿自动化个人数据系统咨询委员会（US Secretary's Advisory Committee on Automated Personal Data Systems）在 1973 年的题为《录音、计算机与公民权利》（Records，Computers，and the Rights of Citizens）的报告中提出了公平信息实践原则（FIPPs），此后美国

FTC（Federal Trade Commission，FTC）的 FIPPs 被广泛接受为公平信息的准则，也成为美国联邦贸易委员会执法活动的重要指引，同时成为全球公认的数据保护制度的理论基石。

从其起源开始，FIPPs 在不断被修订完善，相关原则主要指以下几个方面：

一是透明性原则，组织应该在收集、使用、传播和维护个人可识别信息方面保持透明，并告知用户。

二是个人参与原则，组织应该在可行的条件下让个人尽可能参与到使用个人可识别信息的过程中，寻求个人对收集、利用、传播和维护个人可识别信息的认可。组织还应该提供恰当的访问、纠正、重置有关个人可识别信息使用的机制。

三是明确用途原则，组织应该阐明允许收集个人可识别信息的授权，并且阐明用途。

四是数据最小化原则，组织应该仅收集达成具体目的所需的直接相关且必要的个人可识别信息，并仅保留能够达成具体目的所需要的必要时限。

五是使用限制原则，组织应该仅将个人可识别信息用于通告中阐明用途，共享个人可识别信息与收集个人可识别信息。

六是数据质量和完整性原则，组织应在可能的情况下确保个人可识别信息准确、相关、及时和完整。

七是安全性原则，组织应当通过恰当的安全防护措施保护个人可识别信息（所有媒体上的），抵御丢失、非法访问或使用、毁坏、修

改、意外或不恰当泄露等风险。

八是责任和审计原则，组织应当为遵守这些原则负责，给所有使用个人可识别信息的雇员和分包商提供培训，并对个人可识别信息的实际使用进行审计，以证明遵守了这些原则和所有可适用的隐私保护要求。

3．数据保护的具体制度

收集使用数据规则

联邦和州一级的隐私和数据保护法律组成了美国保护个人信息的立法框架。

收集和使用数据的相关规则包含在各领域的联邦法律中，其中包括：1974 年《隐私法》适用范围仅为联邦政府部级、委员会以上级别的机构收集处理个人信息，要求政府机关向个人告知在他或她身上的任何记录。其次，它要求机构在收集和处理个人信息时遵循一定的原则，即“公平信息惯例”。针对私营组织，美国法律通常规定收集使用数据必须得保护个人隐私且让用户知情，如《金融服务现代化法》的规定金融机构必须制定预防措施防止透露用户个人信息，且必须向新用户告知其信息共享的政策，1984 年《有线电视隐私法》（Cable TV Privacy Act of 1984）规定了在有线电视领域的隐私保护，如个人信息的收集使用的情况需让用户知情。但是某些领域如儿童在线隐私、医疗、教育等特殊领域对监管客体施加了更强的隐私保护义务。《儿童在线隐私保护法》特别保护 13 岁以下儿童的隐私权，收集或使用其

的任何个人信息，必须征得父母同意。《健康保险便利及责任法》的隐私规则规定了医疗信息中个人权利的联邦授权，对个人识别健康信息的使用和披露施加了限制，并规定了对违法行为的民事和刑事处罚，补充的安全规则包括以电子形式保护健康信息的标准。《家庭教育权利和隐私法案》（The Family Educational Rights and Privacy Act，FERPA）禁止教育机构在未经学生或未成年人的学生父母书面同意的情况下披露“个人身份识别信息”，不遵守 FERPA 的学校有可能失去联邦资助。

在特定的监管环境之外，美国的数据收集，使用和共享限制通常是通过公司的隐私政策自行实施的。遵守隐私政策中的表述受到州和联邦级别的消费者保护法的约束。这些自律框架具有问责制和执行部分，越来越多地被用作监管者执行的工具。联邦贸易委员会依据 FTC 法第 5 条给相关公司提起了许多执法行动.

企业数据保护义务

针对企业的个人信息保护义务，主要在是针对私营领域分行业、分领域立法保护中有所体现，企业对应的数据保护义务主要是体现在 FTC 与 FCC 的执法中。其中 FTC 作为综合类、跨行业的隐私保护执法机构，采用多种执法手段来保护消费者隐私和个人数据。其中最主要的工具是通过执法行动停止违法行为，要求企业采取切实的措施来纠正违法行为。FTC 的执法手段对应的企业的义务包括：一是企业需执行全面的隐私和安全计划；二是企业需聘请独立专家定期进行相关评估；三是企业侵犯用户权力后对用户进行经前赔偿，退还不法所得；

四是企业需删除非法获取的用户信息；五是企业需给用户提供明确的通知和选择机制；六是企业保留记录与合规报告。

数据跨境传输规则

美国除部分政府信息存储要求之外，没有跨境数据流动方面的法律限制。美欧安全港是美国商务部与欧委会签订的关于解决美欧之间数据跨境流动问题的安全协议。加入该协议的公司资源遵守欧盟有关数据保护的法规以及安全港协议中确定的数据保护的七项原则。2015 年 10 月欧盟法院做出判决，美欧数据保护港机制失效，历经 15 年的美欧安全港丧失合法性基础，美国企业自此无法再依据该框架实现合法的跨境数据传输。

数据泄露通知制度

美国是最早应用数据泄露通知制度的国家，其立法更加注重对个人的身份盗用治理，对涉及泄露的“个人信息”范畴进行了明确的界定。美国在联邦层面并未出台数据泄露通知相关立法，该项制度最早确立于加利福尼亚州 2002 年颁布的“安全泄露通知法案”中，并逐渐为各州立法所吸收，截止 17 年 6 月目前已有 48 个州建立了数据泄露通知制度。

（二）欧盟数据保护法律制度

1．数据保护立法概况

欧盟是目前世界上数据保护立法较为先进的地区。1995 年，欧

盟即通过了“数据保护指令”（95/46/EC）。2016 年 4 月，欧盟发布了“通用数据保护条例”（以下简称 GDPR），对于个人数据权利、数据控制者的数据保护义务等进行了创设性的规定。除数据保护一般性的规定外，针对具体行业，欧盟也出台了相关的数据保护规定，如针对通信领域的数据保护出台了 ePrivacy 指令等。

2．数据保护的原则

欧盟在立法中确立了如下的数据保护原则：一是合法、公正、透明原则，对个人数据进行合法、公正、透明的处理；二是目的限制原则，必须根据特定的、明确的、合法的目的收集个人数据。允许为公共利益、历史研究或统计的目的而收集个人数据；三是最小数据原则，为达到原始目的收集充分的、相关的、有限的数据；四是精确原则，应当采取有效促使保障个人数据的准确、及时，并及时对不准确的信息进行删除或修正；五是存储限制原则，个人数据存储的形式能够识别数据主体的程度不得超过数据处理目的的必要；六是完整、保密原则，数据处理过程中，应当对数据保护采取适当的保障措施，包括采取技术的、组织的措施防止对个人数据未经授权的或非法的处理、意外损失、破坏或损坏等。

3．数据保护的具体制度

收集使用数据规则

（1）个人数据合法处理规则

根据 GDPR 的规定，合法处理数据应当至少满足下列一项：a.数据主体同意根据某些特定目的处理其个人数据；b.为履行合同的需要而必须处理个人数据，数据主体是合同一方或数据处理是数据主体加入合同的前提；c.数据处理是数据控制者遵守法定义务的需要；d.数据处理是保护数据主体或其他自然人重要权益的必要；e.数据处理是为实现公共目的，或是官方部门赋予数据控制者的权限；f.数据处理市委数据控制者或第三方的合法权益，但此权益不可超越数据主体的基本权益和自由。

（2）个人数据处理获得同意规则

基于数据主体同意而处理个人数据的，数据控制者应当能够证明已经获取了数据主体的同意。在获得用户同意方面，GDPR 增加了对于儿童的特别规定，必须获得监护人的授权或同意。

（3）特殊类别个人信息的处理

GDPR 第 9 条规定了对于特殊类别的个人数据的保护。涉及民族或种族、政治观点、宗教信仰、工会成员、性生活或性取向、基因数据、生物数据等，能够识别特定自然人的数据禁止处理。

（4）与违法犯罪相关的个人数据处理

GDPR 借鉴了“数据保护指令”中关于犯罪记录相关个人信息的规定，只有经过有权机关或欧盟、成员国法律的规定才能处理。

企业数据保护义务

（1）数据控制者的义务

数据控制者应当采取技术、组织和政策措施保障数据处理遵守

GDPR 的规定，并制定相关行为规范（第 40 条），建立认证机制（第 42 条）。对数据处理活动进行记录（第 30 条），发生个人数据泄露时，在 72 小时内立即上报监管部门（第 33 条）。在数据处理采取新技术之前，数据控制者应当对数据处理可能对数据保护产生的影响进行评估（第 35 条）。

（2）数据处理者的义务

“数据处理者”应当履行的义务包括：保持文档充分；实施安全标准；实施日常数据保护影响评估；设置数据保护专员；数据跨境流动的规则；与国家数据监管机构合作等。不遵守规定将会受到处罚和损害赔偿。

数据跨境传输规则

欧盟数据向美国转移主要通过美欧“安全港”协议来规制。GDPR 未对“数据保护指令”中关于数据跨境的规定进行实质性的更改，只是增加了违反相关规定的罚款数额。向欧盟以外的国家转移数据必须满足 GDPR 规定的条件，包括：（1）遵守 GDPR 的规定；（2）欧委会认定被传输数据的第三国或地区、国际组织能够对个人数据进行充分的保护；（3）对个人数据提供安全保障，并对数据主体的权利提供有效的法律救济。

数据泄露通知制度

（1）向数据保护监管部门报告数据泄露

数据控制者发现数据泄露，应当在 72 小时内及时告知数据保护监管部门。但不会对自然人的权益和自由造成威胁的数据泄露，可以

不上报监管部门。

（2）告知数据主体数据泄露

当数据泄露可能会对自然人的权益和自由造成高风险时，数据控制者应当立即告知数据主体。

（三）我国数据保护法律制度

1．数据保护立法概况

伴随着网络信息的技术的高速发展，《网络安全法》的发布标志着我国在数据保护领域的法治建设迈进了新的时代。同时，有关数据保护方面的法律法规也在逐步完善。目前，我国数据保护法律法规体系的建设基本采用“渗透型”模式，即国家没有独立制定数据保护基本法，而是把涉及数据保护的立法思想渗透到其他相关的法律法规、部门的规章和司法的解释之中。

法律法规

我国立法中包含了数据保护相关内容的法律主要有：《中华人民共和国宪法》、《中华人民共和国刑事诉讼法》、《中华人民共和国刑法》、《中华人民共和国治安管理处罚法》、《中华人民共和国行政处罚法》、《中华人民共和国国家安全法》、《中华人民共和国人民警察法》、《中华人民共和国网络安全法》《中华人民共和国电子签名法》、《中华人民共和国保守国家秘密法》、《中华人民共和国专利法》、《中华人民共和国著作权法》、《全国人大常委会关于维护互联网安全的决定》等。

行政法规

行政法规层面，我国在《互联网信息服务管理办法》、《中华人民共和国计算机信息系统安全保护条例》《计算机网络信息国际联网安全保护管理办法》、《互联网上网服务营业场所管理条例》《中华人民共和国电信条例》、《计算机软件保护条例》、《商用密码管理条例》等行政法规中都对数据保护工作进行了规定。

2．数据保护的原则

在《中华人民共和国个人信息保护法（草案)》中明确提出了几项个人信息使用的原则：

合法原则

个人信息的收集、处理和利用应当遵循合法、正当、必要的原则，不得违反法律、法规的规定和双方的约定收集、处理和利用个人信息。

知情同意原则

不符合本法或其他法律、法规规定，或未经信息主体知情同意，不得收集个人信息。收集不需识别信息主体的个人信息，应当消除该信息的识别力，并不得恢复。

目的明确原则

个人信息的收集应当有明确而特定的目的，不得偏离有关目的收集个人信息。不得以欺诈、胁迫等其他不正当的手段获取个人信息。

限制利用原则

个人信息的处理和利用，必须与收集目的一致，必要情况下的目

的变更应当有法律规定或取得信息主体的同意或其他正当理由。

完整正确原则

信息处理主体应当保证个人信息在利用目的范围内准确、完整并及时更新。

安全原则

信息处理主体应当采取合理的安全措施保护个人信息，防止个人信息的意外丢失、毁损，非法收集、处理、利用。

网络运营者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。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

可追溯、可异议、可纠错原则

信息处理主体必须保障个人信息来源渠道和信息使用渠道清晰，确保个人信息可追溯、可异议和可纠错。

3．数据保护的具体制度

我国的数据保护不像欧美等国家法律从具体层面给出了指导意见，从目前已有的法律条文来看明确了一下几条具体的保护措施：

明确管理职责

《网络安全法》赋予了电信主管部门管理网络数据的职权和责任，是电信主管部门电信和互联网网络数据管理工作“有位有为有声”的基础。同时，构建了涵盖管理依据、管理细则、管理手段、执法机制

的网络数据管理体系。如《网络安全法》明确指出：国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

明确管理重点环节

综合《网络安全法》和工信部文件，将网络数据管理的重点环节确定为“采集、传输、存储、使用”，每个环节都包括多种与数据相关的行为。

网络数据管理的重点环节的标准为：一是是否涉及数据的流动（从一处到另一处）；二是是否涉及主体关系的产生、变化。采集和使用环节是管理的重点，其中采集环节的核心在于保障用户的知情权和选择权，而使用环节的核心则是对数据境内外流动行为做出行为规范，境内流动（公开、共享、采集）重点关注在鼓励的前提下明确责任，境外流动重点关注数据主权。

执行等级保护制度

网络安全法明确：网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

完善预警监测机制建立应急响应处置

国家将建立安全监测预警及信息通报制度，行业监管部门也要建立相应的通报制度，形成网络事件逐级上报的机制。

联系我们：

数据中心联盟

地址：北京市西城区月坛南街 11 号

邮箱：shilin1@caict.ac.cn

联盟网站：http://www.dca.org.cn/