龙华区
企业数据合规建设
实务指南

中共深圳市龙华区委宣传部
2025 年 7 月

龙华区
企业数据合规建设
实务指南

中共深圳市龙华区委宣传部

2025 年 7 月

总策划：黄立敏

总　编：吴　江　张　煦

编　委：范　超　赵振动　刘大亮　张　巍
肖赛尔　吴港澳

目　录

前　言

龙华区把“数字经济·都市核心”作为战略目标，坚持数字产业化、产业数字化、治理数字化、数字价值化理念，打造数字经济、数字城区、数字治理“三位一体”的数字龙华战略路径。区内企业数据资源丰富，数据价值优势突出，随着数字经济快速发展，各类数据加速流通，数据合规问题日益凸显，企业的数据合规管理需求更加迫切。

为规范龙华区企业的数据合规管理，区委宣传部（网信办）于2023年8月启动了企业数据合规专项调研工作，调研范围覆盖了电子商务、人工智能、金融科技、快递物流等不同领域的30余家企业。调研发现企业普遍存在数据合规风险意识不强、合规管理机制不健全、合规技术措施不完善等问题。

围绕调研发现的问题，区委宣传部（网信办）组织数据合规多个领域的专家研究应对策略，并区分不同维度分类汇总，于2024年9月发布了《龙华区企业数据合规建设指引手册》。该手册从法律、管理、技术等多维度为企业介绍了数据合规建设的相关知识，助力企业明晰数据合规建设方向和工作重点。

在发布和宣贯指引手册的同时，区委宣传部（网信办）选取了部分具有代表性的试点企业，以《龙华区企业数据合规建设指引手册》为纲领开展企业数据合规建设实践探索。在实践过程中，部分企业遇到了合规义务难以识别、数据分类分级标准模糊、跨部门协作效率低等难题。区委宣传部（网信办）及时协调专家团队，通过一对一指导、定期座谈会等方式，协助企业梳理数据资产，识别数据合规管理义务，制定数据分类分级规则，建立跨部门数据合规协同机制。经过持续优化改进，我们欣喜地看到，试点企业构建起了基础的数据合规管理体系，不

仅有效降低了数据泄露、违规使用等风险，还通过规范数据管理促进了业务发展，实现了数据安全与业务发展的双赢。

为了惠及更多企业，推广实践探索成果，我们编写了《龙华区企业数据合规建设实务指南》。本实务指南系统地呈现了企业数据合规建设的实践工作流程与要点，包含识别数据合规管理义务、建立数据合规管理体系、完善数据安全技术措施、关注数据合规重点工作、运用数据合规建设成果等内容，是对《龙华区企业数据合规建设指引手册》内容的进一步深化与落地。

希望《龙华区企业数据合规建设实务指南》能为龙华区企业提供更具实操性的指导，帮助企业在数据合规建设的道路上少走弯路，切实提升数据合规管理水平，充分释放数据价值，在数字经济的赛道上稳健前行，为建设“数字龙华、都市核心”注入更强劲的动力，共同开创龙华区数字经济发展的新局面。

本实务指南可以帮助企业以下人员：

企业主要负责人：助力企业高层全面洞察数据合规建设对企业战略布局的深远影响。通过了解不同业务场景下的数据合规要求，在制定企业发展战略、拓展新业务领域时，能够前瞻性地规划数据合规路径，确保企业发展方向与数据合规要求高度契合。

企业数据合规管理人员：为数据合规管理团队提供有指导性、可操作的数据合规管理体系建设蓝图。从识别数据合规管理义务入手，到建立数据合规管理组织、制定全面的数据合规管理制度，再到规范数据合规运营过程，每个环节都有具体实践指导，帮助管理团队构建一套贴合企业实际的数据合规管理体系。

企业数据合规技术人员：实务指南详细介绍了数据安全技术控制措施和常见工具，包括加密技术、脱敏技术、访问控制技术、数据备份与恢复技术等。技术人员能够全面了解这些技术的应用场景，优化技术选型和架构设计，为企业提供科学合理的数据合规建设方案和技术路径决策支持。

导　读

《龙华区企业数据合规建设实务指南》旨在为企业提供可落地的实践指南，助力企业应对数字经济发展中的数据合规挑战。本实务指南围绕企业数据合规建设全流程，系统整合实践经验与专业知识，从合规义务识别到合规成果运用形成完整闭环，切实帮助企业提升数据合规管理水平，释放数据价值。《龙华区企业数据合规建设实务指南》包括五个章节和两个附录：五个章节分别针对企业数据合规建设实践过程的五个阶段进行介绍；附录一是对实务指南内容中使用的专业术语的释义；附录二是指南内容所引用的法律法规及标准索引。

第一章识别数据合规管理义务：本章节将介绍企业识别数据合规管理义务的具体方法与流程。从组建数据合规治理工作小组入手，深入梳理业务场景和数据处理流程，组织数据资产分类分级，确定适用的法律法规和监管要求，明确数据合规管理义务，评估数据合规风险，并最终形成数据合规管理共识。这个阶段的工作是企业数据合规管理的基础性工作，决定了企业数据合规管理工作要投入的资源和预期达成的目标。

第二章建立数据合规管理体系：本章节将探讨如何构建有效的数据合规管理体系。企业应全面收集整理现有数据合规管理相关制度文件，进行制度合规性审查，分析现有制度的优势与不足。基于分析结果和企业自身特点设计管理组织架构和组织工作机制，确保各级组织分工明确，资源配置充分，沟通协作通畅。同时，通过设计合理的制度体系结构和编制制度文件，确保各项制度之间相互协调、相互支撑，为企业的数据合规管理工作提供有力的制度保障。

第三章完善数据安全技术措施：本章节将分析如何分步骤完善数据安全技术措施。通过对企业现有数据资产、网络架构、安全漏洞等方面进行全面且细致的评估，清晰掌握数据安全的当前状况。依据评估结果，结合企业业务需求和发展战略，制定出贴合实际的、具有前瞻性的数据安全策略与方案。按照规划有序部

署各类数据安全技术，逐步形成完善的数据安全技术体系，支撑数据合规管理体系的有效落地。

第四章关注数据合规重点工作：本章节将聚焦于数据合规管理中的一些重点工作。网络安全等级保护为企业数据合规运营筑牢安全防线，抵御外部网络攻击与威胁；重要数据识别与管理则帮助企业有效管理重要数据和核心数据，守护国家安全与自身核心利益。个人信息保护影响评估和合规审计，致力于保障个人信息安全，维护用户信任。数据出境合规管理确保企业在全球化进程中，数据跨境流动合法有序。生成式人工智能应用合规管理使企业在享受技术红利时，遵循道德与法律边界。这些重点工作相互关联、相辅相成，共同构建起企业数据合规管理的完整体系，是企业实现可持续发展的必要保障。

第五章运用数据合规建设成果：本章节将阐述数据合规建设成果对企业的积极影响。企业通过前期在识别数据合规管理义务、建立合规组织、制定管理制度、完善安全技术措施以及规范运营过程等方面的不懈努力，积累了丰富的数据合规建设成果。如何充分运用这些成果，对于维护企业合法权益、提升企业品牌形象、实现数据资产入表、促进数据产品交易、拓展和创新业务具有深远意义。

附录一《专业术语释义》：汇总实务指南中涉及的数据合规领域专业术语，涵盖法律概念、技术名词、管理术语等。通过精准释义，帮助企业人员尤其是非专业岗位人员消除理解障碍，确保在阅读实务指南及开展数据合规工作时，对关键概念形成统一认知，避免因术语歧义导致执行偏差。

附录二《法律法规及标准索引》：汇总实务指南中引用的法律法规及标准，将其区分已生效文件和未生效文件，整理罗列了文件名称、颁布时间、实施时间、颁布机构等，以便于企业查询。需要注意的是，其中未生效的文件引用入实务指南，仅供企业参考以说明监管趋势，该等文件生效版本可能与未生效版本存在较大差异，特别提请各企业持续关注各文件相关的发布动态。

第一章 识别数据合规管理义务

识别企业数据合规管理义务是企业数据合规管理工作开展的第一步，也是基础性工作，决定了企业数据合规管理工作要投入的资源和预期达成的目标。本章节将介绍企业识别数据合规管理义务的具体方法与流程，从组建数据合规治理工作小组入手，深入梳理业务场景和数据处理流程，组织数据资产分类分级，确定适用的法律法规和监管要求，明确数据合规管理义务，评估数据合规风险，并最终形成数据合规管理共识。

（一）组建数据合规治理工作小组

数据合规治理涵盖了从宏观战略规划到微观业务执行的各个层面，需要整合多领域的专业知识与技能。因此，一个结构合理、职责清晰、具备专业素养的工作小组，就成为了企业有效开展数据合规工作的核心支柱。下面，我们将详细阐述组建数据合规治理工作小组的具体步骤和注意事项。

1. 明确工作小组的定位与目标

数据合规治理工作小组的主要任务是确定企业的数据合规工作范围、战略方向、政策框架和整体目标，指导企业建立数据合规管理组织和制度体系。在企业数据合规管理体系发布之前对企业数据合规工作负责。

在明确了定位之后，应制定具体、可量化且切实可行的工作目标。比如，设定在未来 3 个月内，要完成对企业数据合规现状的全面、深入评估；在半年内，成功建立一套贴合企业实际情况的全方位数据合规管理体系；并且通过持续不懈的合规努力，将数据泄露、违规操作等风险事件的发生概率降低到一个可接受的较低水平。

2. 确定工作小组的成员构成

企业可充分考量组织内现有成员和外部相关资源，根据企业业务特点和数据处理活动复杂性决定工作小组成员构成，可以考虑在以下几类人员中选取：

（1）高层领导代表：企业的高层领导，如首席执行官（CEO）、首席财务官（CFO）、首席信息官（CIO）等。可以在企业高层领导中选择一至数位代表，他

们站在企业战略的高度，能够为数据合规工作提供强有力的支持。不仅可以调配企业内部的各种必要资源，还能有效地协调各部门之间的关系，确保数据合规工作与企业的整体运营目标紧密契合。举例来说，CEO 可以在资源的分配上给予大力支持，确保合规工作所需的人力、物力和财力得到满足；而 CIO 则能凭借其在企业信息技术战略方面的专业知识，为数据合规工作提供独特而有价值的见解。

（2）法务专家：精通数据保护相关法律法规的法务人员是工作小组中不可或缺的重要成员。他们熟悉国内外数据法规的变化动态，具备对法律条文清晰准确地解读能力。在企业制定数据管理政策时，他们能够依据《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》等重要法律法规，审查企业数据管理政策的合法合规性，提出专业的法律意见和建议。

（3）合规管理人员：专业的合规管理人员具备制定和实施企业合规管理制度的工作经验。他们可以帮助企业评估合规风险，提供合规管理体系建设建议，协助建立合规管理制度、流程和标准，还可以对企业内部各部门执行数据合规要求的情况进行全方位的监督，帮助企业及时发现潜在的合规问题，并给出有效的纠正措施建议。

（4）业务部门负责人：企业各个业务部门，如销售、市场、运营、研发等部门的负责人，在工作小组中发挥着关键作用。他们对本部门的业务流程和数据使用场景了如指掌，能够详细地提供关于数据产生、收集、处理和流转的具体信息。这些信息对于工作小组制定符合实际业务需求的合规策略至关重要。

（5）信息技术专家：网络安全工程师、数据安全工程师、系统架构师、数据库管理员等在内的信息技术专业人员，可以在企业数据安全和合规建设方面给予专业技术支持。他们可以对企业现有数据系统的安全性和合规性进行全面评估，给出数据安全技术措施建议。

（6）内部审计人员：内部审计人员在企业中具有独立、客观的监督作用。

他们独立于企业的其他部门，可以按照严格的审计标准和流程，对数据合规工作进行全面审查。通过提供专业的数据合规审计建议，参与数据合规审计相关制度的制定，确保企业的数据合规工作得到有效执行，不出现工作疏漏。

（7）数据保护官：数据规模较大或者数据处理活动较为复杂的企业设立有数据保护官。数据保护官全面负责协调企业内部的数据保护工作，确保各个部门之间的信息共享和协作能够顺畅进行。同时，他们作为企业与监管机构沟通的重要桥梁，负责处理数据主体的相关请求和投诉，维护企业与数据主体之间的良好信任关系，在企业的数据合规治理中发挥着关键的协调和沟通作用。

（8）外部顾问：为了使工作小组能够接触到更广泛的专业知识和行业经验，邀请数据合规领域的外部专家、咨询顾问或行业协会代表作为外部顾问加入工作小组是一个明智的选择。他们凭借丰富的行业经验和专业知识，能够为工作小组带来行业内的最新动态、最佳实践经验以及先进的合规趋势。同时，他们还能提供专业的技术支持，为企业的数据合规治理提供更广阔的视野和更深入的专业指导，帮助企业提升数据合规治理水平。

龙华区委宣传部（网信办）为了给区内企业解决数据合规建设道路上的各种“疑难杂症”，联合数据合规领域的权威机构以及优质企业，组建了一支高水平的数据合规专家顾问小组，他们可以从多个方面为区内企业带来全方位、专业化的免费咨询服务。具体内容可登录“i 龙华”小程序，进入“虚拟园区”的“找政务”板块，点击“企业公共关系服务平台”了解详情。

3. 明确工作小组成员的职责与分工

数据合规治理工作小组成立后，应根据人员岗位权限和专业能力确定成员职责和分工，可以参考以下基本思路：

（1）决策与支持：高层领导代表在工作小组中主要负责制定数据合规的战略方向。他们需要综合考虑企业的整体发展目标、市场竞争环境以及法律法规要求等多方面因素，作出科学合理的决策。对于重大的合规决策，他们要进行严格的审批，确保决策的正确性和可行性。同时，他们还需要负责协调企业内部的各种资源，为数据合规工作的顺利开展提供有力支持。在平衡数据合规的成本与效益方面，他们负责把握尺度，确保合规工作与企业的商业目标相互协调，实现企业的可持续发展。

（2）法规解读与合规审查：法务专家的核心职责是深入解读数据保护法律法规、政策文件，确定与企业相适用的法律法规与监管要求，及时将新的法规要求传达给工作小组的其他成员。在企业的数据治理活动中，他们负责对每一个工作环节进行严格的法律合规审查，提供专业的法律意见和建议，确保企业在法律的框架内开展数据治理活动，避免出现源头性的法律风险。

（3）风险评估与制度建设：合规管理人员负责制定和完善企业的数据合规管理制度和流程。他们负责依据已确定的与企业相适用的法律法规与监管要求，结合企业的数据处理流程和数据敏感级别，评估企业数据合规管理风险，明确数据合规管理义务，并根据企业的实际情况制定出一套切实可行的制度体系。

（4）业务场景梳理与合规实施：业务负责人负责将企业的业务需求与数据合规要求紧密结合起来，根据工作小组需要梳理业务场景。在制定数据合规方案时，他们要充分发挥自己对业务的熟悉优势，提供详细的业务信息和实际需求。同时，负责积极推动合规措施的落实，确保每一位员工都能理解和遵守数据合规要求。在业务执行过程中，如果遇到任何合规问题，他们要及时反馈给工作小组，为小组决策提供准确的依据，促进合规方案不断优化。

（5）技术保障与安全防护：信息技术专家负责结合业务场景梳理数据处理流程，识别数据资产，组织数据资产的分类分级，并为合规管理人员执行合规风

险评估提供技术保障，对企业数据系统的安全风险进行全面评估。他们要运用专业的技术手段，分析系统可能存在的漏洞和隐患。根据评估结果，协助合规管理人员制定数据安全技术方案，包括加密技术的应用、访问控制机制的建立、数据备份与恢复系统的完善等。

（6）审计策划与实施：内部审计人员负责数据合规审计的策划与实施，结合《个人信息保护合规审计管理办法》等数据合规审计相关法律法规和监管要求，协助工作小组制定数据合规审计相关管理制度，明确审计工作的目标、原则、职责分工等关键内容，确定审计范围、审计对象和审计频次。同时，负责设计审计工作流程，涵盖审计计划的制定、审计项目的实施、审计报告的撰写与提交、审计发现问题的整改跟踪等各个环节，确保数据合规审计工作有序、高效开展。

（7）协调与沟通：数据保护官负责建立有效的沟通机制，确保部门之间的信息能够及时共享，协作能够顺畅进行。同时，作为企业与监管机构沟通的代表，他们要及时了解监管机构的要求和动态，向监管机构汇报企业的数据合规工作情况。在处理数据主体的权利请求和投诉时，他们要以专业、负责的态度，及时有效地解决问题，维护企业与数据主体之间的良好关系。

（8）专业指导与经验分享：外部顾问负责为工作小组提供专业的指导和建议。他们可以分享行业内的数据合规最佳实践案例，介绍最新的合规技术和方法。在企业遇到复杂的合规问题时，他们能够提供独特的解决方案，帮助企业提升数据合规治理水平。同时，他们还可以为工作小组的成员提供培训，促进成员之间的知识交流和共享。

4. 建立工作机制

数据合规治理小组成立后，必须建立相适应的工作机制，以保障组织的高效运行，这些工作机制包括但不限于以下内容：

（1）会议机制：建立一套完善的定期工作小组会议制度是非常必要的。可以设定每周或每月召开一次例会，在例会上，小组成员们共同讨论工作的进展情况，分享工作中遇到的问题和解决方案，部署下一步的工作任务。同时，根据工作的实际需要，随时召开临时会议，以应对突发的合规事件或需要紧急作出的决策。通过会议制度，确保工作小组的信息能够及时共享，决策能够迅速做出，工作能够有序推进。

（2）沟通机制：明确工作小组内部及与企业其他部门之间的沟通渠道和方式是提高工作效率的关键。可以利用内部邮件系统、即时通讯工具、项目管理软件等多种方式进行沟通。确保信息能够及时、准确地传递，避免出现信息不对称的情况。同时，建立良好的沟通氛围，鼓励成员之间积极交流，分享经验和想法，促进各成员之间的协作与配合。

（3）决策流程：制定清晰、明确的决策流程是保证工作小组决策科学性和公正性的重要保障。对于一般性的合规问题，可以由工作小组组长或相关负责人根据自身专业知识和经验直接作出决策。对于重大的合规决策，则需要经过工作小组全体成员的充分讨论和审议，广泛听取各方的意见和建议。在讨论的基础上形成初步决策方案，然后提交企业高层领导进行最终审批。通过这样的决策流程，确保决策的质量和可行性。

（4）汇报机制：建立定期的工作汇报制度，工作小组要按照规定的时间和要求，向企业高层领导汇报数据合规工作的进展情况、存在的问题以及提出的解

决方案。通过工作汇报，让高层领导及时了解数据合规工作的动态，为高层领导的决策提供依据。同时，各成员之间也需要定期汇报各自负责的工作内容，确保工作小组对整体工作有全面、深入地了解，及时发现问题并进行调整。

一个职责明确、协同高效的数据合规治理工作小组将为企业后续的数据合规管理工作提供坚实的组织保障，支持企业完成数据合规义务识别、数据合规组织搭建和数据合规制度制定各阶段的工作。

（二）梳理业务场景与数据处理流程

企业要实现有效的数据合规管理，首先需要全面、深入地梳理业务场景与数据处理流程。这不仅是识别数据合规义务的起点，更是确保数据在整个生命周期内合法、安全、有效利用的基础。以下将详细阐述梳理业务场景与数据处理流程的具体步骤。

1. 全面收集业务信息

数据治理工作小组需通过多种方式全面收集企业的业务信息。一方面，与各业务部门负责人和一线员工进行访谈，了解各业务环节的具体操作流程、业务目标以及数据在业务中的作用。例如，在客户关系管理业务中，了解销售团队如何获取潜在客户信息、跟进客户过程中记录哪些数据以及这些数据对销售决策的影响。另一方面，查阅企业的业务文档，如业务流程手册、操作指南、项目方案等，获取书面的业务描述和数据相关信息。此外，观察实际业务操作也是收集信息的有效方式，能够发现一些在文档和访谈中未被提及的细节。

2. 绘制业务场景图

在收集到足够的业务信息后，工作小组开始绘制业务场景图。业务场景图以可视化的方式呈现企业的各项业务活动及其相互关系。可以按照业务的功能模块或流程顺序进行绘制，每个业务场景用特定的图形或符号表示，并标注关键业务环节和数据流动方向。例如，对于电商企业的订单处理业务场景，业务场景图可展示从用户下单、订单审核、库存检查、支付处理到发货配送等环节，以及每个环节涉及的数据输入和输出。通过绘制业务场景图，能够直观地了解企业业务的全貌，为后续的数据处理流程梳理提供清晰的框架。

3. 梳理数据处理流程

数据处理活动包括收集、传输、存储、加工、交换、销毁等多个环节，可以结合业务场景分环节梳理出数据处理流程。必要时，可以绘制数据处理流程图，以便于更清晰地了解数据处理全过程：

（1）数据收集环节：分析数据是如何从产生源头被收集到企业的信息系统中的。可能涉及人工录入、系统自动采集、接口对接等多种方式。例如，企业通过网站表单收集用户注册信息，通过 API 接口从合作伙伴处获取业务数据。了解数据收集的方式和渠道，便于评估数据收集过程中的合规风险。

（2）数据传输环节：分析数据在企业内部不同系统之间以及与外部合作伙伴之间的传输方式和路径。考虑数据传输过程中的安全性，如是否采用加密传输协议，防止数据在传输过程中被窃取或篡改。

（3）数据存储环节：确定数据存储的位置和方式，包括数据库类型（如关系型数据库、非关系型数据库）、存储设备（本地服务器、云存储等）。同时，

关注数据存储的安全性和备份策略，确保数据的完整性和可用性。

（4）数据处理环节：梳理数据在系统中经过的各种处理操作，如数据清洗、转换、分析、挖掘等。例如，数据分析部门对销售数据进行统计分析，以生成销售报表和市场趋势预测。明确数据处理的算法和逻辑，有助于评估数据处理的合法性和合理性。

（5）数据交换环节：明确数据在企业内部的使用目的和范围，以及数据是否被共享给第三方。例如，企业将客户数据用于精准营销，同时可能根据合作协议将部分数据提供给广告合作伙伴。了解数据使用情况，能够发现潜在的数据合规问题，如数据滥用、未经授权的共享等。

（6）数据销毁环节：确定数据在达到一定保存期限或不再有使用价值时的销毁方式和流程。确保数据销毁符合法律法规要求，避免敏感数据泄露。

4. 审核与完善

完成业务场景和数据处理流程的初步梳理后，工作小组需对梳理结果进行审核。审核过程中，检查业务场景图和数据处理流程是否准确、完整地反映了企业的实际业务和数据处理活动，是否存在遗漏或错误。可以通过再次与业务部门人员沟通、进行实际业务验证等方式进行审核。根据审核结果，对梳理结果进行完善和修正，确保业务场景和数据处理流程的准确性和可靠性。

（三）组织数据资产分类分级

在完成对业务场景与数据处理流程的梳理后，组织数据分类分级成为数据合规管理中至关重要的一环。合理的数据分类分级能够使企业更加清晰地了解自身数据资产，有针对性地采取保护措施，同时满足法律法规和监管要求。数据治理

工作小组应制定整体的数据分类分级原则；法务部门人员从法律合规角度确保分类分级符合相关法律法规；业务部门人员凭借对业务的熟悉，准确界定数据在业务中的重要性和敏感性；信息技术部门人员则提供技术支持，确保数据分类分级在技术上得以有效实现。以下是组织数据分类分级的具体工作步骤：

1. 确定数据分类分级原则

企业应遵循国家数据分类分级保护要求，按照数据所属行业领域进行分类分级管理，可参考以下原则对数据进行分类分级：

（1）科学实用原则：从便于数据管理和使用的角度，科学选择常见、稳定的属性或特征作为数据分类的依据，并结合实际需要对数据进行细化分类。

（2）边界清晰原则：数据分级的各级别应边界清晰，对不同级别的数据采取相应的保护措施。

（3）就高从严原则：采用就高不就低的原则确定数据级别，当多个因素可能影响数据分级时，按照可能造成的各个影响对象的最高影响程度确定数据级别。

（4）点面结合原则：数据分级既要考虑单项数据分级，也要充分考虑多个领域、群体或区域的数据汇聚融合后的安全影响，综合确定数据级别。

（5）动态更新原则：根据数据的业务属性、重要性和可能造成的危害程度的变化，对数据分类分级、重要数据目录等进行定期审核更新。

2. 全面梳理数据资产

结合已经梳理出的数据处理流程，采用“技术扫描+人工核查”的方法，通过查阅数据字典、数据库结构文档、数据使用记录等方式，对企业各类数据（包括结构化/非结构化、生产/归档、自有/第三方）数据进行全面梳理。梳理的对象

包括以电子或其它形式记录的数据表、数据项、数据文件等，梳理内容包括数据内容描述、数据量、保存位置、保存期限、数据处理情况（数据处理目的、数据处理所涉及的信息系统）、数据对外提供情况（提供、转移、公开披露、数据出境）等内容。最后对梳理的结果进行合并，形成数据资产清单。

3. 制定分类分级规则

如企业所在行业领域主管部门已制定行业领域数据分类分级规则，企业应优先按照行业领域数据分类分级规则细化执行，如所属行业领域没有行业主管部门认可的数据分类分级标准规范的，或存在行业领域规范未覆盖的数据类型，企业可参考 GB/T43697-2024《数据安全技术数据分类分级规则》并结合自身实际情况制定数据分类分级规则。

4. 实施数据分类分级

数据分类是为了便于数据管理和使用，数据分级是为了保护数据安全，数据分类分级一般采用先分类再分级的方法。

（1）数据分类

企业数据分类可根据数据管理和使用需求，结合已有数据分类基础，选择业务属性将数据细化分类。常见业务属性包括但不限于：

①业务领域：按照业务范围、业务种类或业务功能进行细化分类。

示例：

金融行业：信贷数据、支付数据、保险理赔数据；

制造业：供应链数据、生产设备数据、产品质检数据；

互联网行业：用户行为数据、广告投放数据、电商交易数据。

②责任部门：按照数据管理部门或职责分工进行细化分类。

示例：

人力资源部：员工档案数据、考勤数据、绩效数据；

财务部：财务报表数据、发票数据、预算数据；

IT 部：系统日志数据、网络安全数据、服务器配置数据。

③描述对象：按照数据描述的对象进行细化分类。

示例：

用户数据：姓名、手机号、消费偏好；

业务数据：订单号、商品 SKU、交易金额；

经营管理数据：战略规划文档、组织架构图、KPI 指标；

系统运维数据：服务器 CPU 利用率、数据库错误日志、网络流量数据。

④流程环节：按照业务流程、产业链环节进行细化分类。

示例：

能源行业：探勘（地质勘探报告）、开采（钻井参数）、生产（炼油厂产量）、加工（成品油质量数据）、销售（客户订单）、使用（用户能耗数据）；

制造业：研发（产品设计图纸）、采购（供应商报价）、生产（工序工时记录）、质检（产品合格率）、仓储（库存位置数据）、物流（运输轨迹数据）。

⑤数据主体：按照数据主体或属主进行细化分类。

示例：

公共数据：政府公开的行业统计数据、气象数据；

组织数据：企业内部的合同文件、研发专利、供应链协议；

个人信息：姓名、电话、身份证号、医疗健康数据、社交媒体账号信息。

⑥内容主题：按照数据描述的内容主题进行细化分类。

示例：

市场营销：客户画像数据、广告点击率、市场调研报告；

研发创新：实验数据、专利文档、技术白皮书；

合规管理：监管政策文件、审计记录、合规检查清单。

⑦数据用途：按照数据处理目的、用途进行细化分类。

示例：

风控用途：信用评分模型数据、欺诈交易识别规则；

客户运营：个性化推荐算法数据、用户分群标签；

合规用途：数据跨境传输审计日志、数据合规性报告。

⑧数据处理：按照数据处理活动或数据加工程度进行细化分类。

示例：

原始数据：传感器实时采集的温度/湿度数据、用户注册表单原始字段；

加工数据：清洗后的客户标签数据、聚合后的销售日报表；

分析数据：用户生命周期价值预测模型、市场趋势分析报告。

⑨数据来源：按照数据来源、收集方式进行细化分类。

示例：

系统产生：ERP 系统订单数据、CRM 系统客户沟通记录；

外部采集：第三方 API（如天气数据、征信数据）、物联网设备（如工厂传感器）；

人工录入：线下纸质表单数字化数据、客服手工录入的投诉记录。

如涉及法律法规有专门管理要求的数据类别（如个人信息等），应按照有关规定和标准进行识别和分类。个人信息分类可参考 GB/T35273-2020《信息安全技术个人信息安全规范》和 TC260-PG-20244A《网络安全标准实践指南—敏感个人信息识别指南》。

（2）数据分级

国家层面，根据数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将数据从高到低分为核心数据、重要数据、一般数据三个级别。

企业在执行数据分级时应该优先识别核心数据和重要数据，识别方法参考GBT43697-2024《数据安全技术数据分类分级规则》附录G重要数据识别指南，然后再对一般数据进行分级。一般数据的分级可参考以下方法：

①一般数据分4级参考：将一般数据从低到高分为1级、2级、3级、4级共四个级别。

1级数据：数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，不会对个人权益、组织权益等造成危害。1级数据具有公共传播属性，可对外公开发布、转发传播，但也需考虑公开的数据量及类别，避免由于类别较多或者数量过大被用于关联分析。

2级数据：数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对个人权益、组织权益造成一般危害。2级数据通常在组织内部、关联方共享和使用，相关方授权后可向组织外部共享。

3级数据：数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对个人权益、组织权益造成严重危害。3级数据仅可由授权的内部机构或人员访问，如果要将数据共享到外部，需要满足相关条件并获得相关方的授权。

4级数据：数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对个人权益、组织权益造成特别严重危害，或对经济运行、社会秩序、公共利益造成一般危害。4级数据按照批准的授权列表严格管理，仅能在受控范围内经过严格审批、评估后才可共享或传播。

②一般数据分3级参考：将一般数据从低到高分为1级、2级、3级共三个

级别。

1级数据：数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对个人权益、组织权益造成一般危害或无危害。

2级数据：数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对个人权益、组织权益造成严重危害。

3级数据：数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对个人权益、组织合法权益造成特别严重危害，或者对经济运行、社会秩序、公共利益造成一般危害。

③一般数据分2级参考：将一般数据从低到高分为1级、2级。

1级数据：数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对个人权益、组织权益造成一般、严重危害或无危害。

2级数据：数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对个人权益、组织权益造成特别严重危害，或者对经济运行、社会秩序、公共利益造成一般危害。

④最低参考级别

一般数据分级应对个人信息、公共数据等特定类型数据设置合理的数据级别，特定类型数据最低参考级别如下。

1)在一般数据分4级框架下，特定类型一般数据的最低参考级别为：

A.敏感个人信息不低于4级，一般个人信息不低于2级；

B.组织内部员工个人信息不低于2级；

C.去标识化的个人信息不低于2级；

D.个人标签信息不低于2级；

E.有条件开放/共享的公共数据级别不低于2级，禁止开放/共享的公共数据不低于4级。

2)在一般数据3级框架下，特定类型一般数据的最低参考级别为：

A.敏感个人信息不低于3级，一般个人信息不低于2级；

B.有条件开放/共享的公共数据级别不低于2级，禁止开放/共享的公共数据不低于3级。

3)在一般数据2级框架下，敏感个人信息不低于2级，禁止开放/共享的公共数据不低于2级。

工作小组应对数据分类分级结果进行审核，形成数据分类分级清单、重要数据和核心数据目录，并按有关程序报送目录。

5. 动态更新

数据分类分级不是一次性的工作，当数据的业务属性、重要程度和可能造成的危害程度变化时通常需要进行动态更新，动态更新常见情形包括但不限于：

（1）数据规模变化，导致原有数据的安全级别不再适用；

（2）数据内容未发生变化，但数据时效性、数据规模、数据应用场景、数据加工处理方式等发生显著变化；

（3）多个原始数据直接合并，导致原有的安全级别不再适用合并后的数据；

（4）因对不同数据选取部分数据进行合并形成的新数据，导致原有数据的安全级别不再适用合并后的数据；

（5）不同数据类型经汇聚融合形成新的数据类别，导致原有的数据级别不再适用于汇聚融合后的数据；

（6）数据进行脱敏或删除关键字段，或者经过去标识化、匿名化处理；

（7）发生数据安全事件，导致数据敏感性发生变化；

（8）因国家或行业主管部门要求，导致原定的数据级别不再适用；

（9）需要对数据安全级别进行变更的其他情形。

6. 数据分类分级标注

在完成数据资产梳理和分类分级评估后，应对数据进行分类分级标注。标注可以在数据存储系统中进行，通过添加元数据标签的方式，明确数据的分类和级别。例如，在数据库表的字段属性中添加“安全级别：4 级”“数据类型：敏感个人信息”等标注信息。同时，建立数据分类分级目录，将标注后的数据按照分类分级结果进行整理和归档，方便企业内部人员查询和使用。

以下是常见的企业数据分类分级标注实现方式：

技术手段	实现方式	适用场景
规则引擎	预设正则表达式（如匹配身份证号、银行卡号），自动标记数据类型和安全级别	结构化数据（数据库字段）
AI 模型	训练 NLP 模型识别文档内容（如合同中的“保密条款”标注“3 级”）	非结构化数据（文档、邮件）
元数据继承	从系统元数据提取标签（如 HR 系统自动标记“员工档案—人力资源部—4 级”）	业务系统内置分类的场景
人工标注平台	提供可视化界面的人工标注方法，支持批量标注与审核	复杂场景（如多维度组合标签）

通过完成数据分类分级工作，企业从“数据混沌”走向“数据有序”，这不仅是合规的要求，更是数据作为生产要素的内在管理需求。

（四）明确数据合规管理义务

基于已经梳理出的业务场景、数据处理流程和数据资产信息，工作小组完成了企业数据处理活动的总体画像。接下来，可以由法务人员、合规管理人员、业务部门代表、专家顾问共同确定企业的数据合规管理义务。法务人员负责解读法律法规；合规管理人员负责跟踪和分析监管动态；业务部门代表则能从实际业务出发，识别与业务相关的合规需求；专家顾问可提供行业特定的法规信息和发展趋势分析。可以参考以下明确数据合规管理义务的工作步骤：

1. 检索相关的法律法规

法律法规检索先从国家层面的法律开始，如《刑法》《民法典》《网络安全法》《数据安全法》《个人信息保护法》等，这些法律对数据的收集、存储、使用、共享等各个环节都有明确规定。接着检索行政法规、部门规章，例如《计算机信息系统安全保护条例》《未成年人网络保护条例》《网络数据安全管理条例》，以及国家网信部门发布的关于个人信息保护、数据安全的管理规定、工信部发布的相关通信管理规定、国家市场监督管理总局出台的关于数据市场监管的规章等。同时，还应关注地方性法规和政策，因为不同地区可能对数据管理有特殊要求，如《深圳特区数据条例》等。

如果企业的业务涉及国际市场，还需检索国际上的数据保护法规。例如，欧盟的《通用数据保护条例》（GDPR），对企业处理欧盟居民个人信息的行为有严格规范；美国的《加州消费者隐私法案》（CCPA）等，也对数据隐私保护提出了

具体要求。了解这些国际法规，有助于企业在跨境业务中避免法律风险。

另外，还要考虑行业监管要求，不同行业有其特定的监管机构和要求。例如，金融行业受中国人民银行、中国银保监会等监管，其对客户金融数据的保护有严格规定；医疗行业则受国家卫生健康委员会等部门监管，涉及患者医疗数据的合规管理。检索行业主管部门发布的监管文件、指引和标准，明确行业内的数据合规要求。

2. 结合业务场景筛选适用的法律法规

将检索到的法律法规与企业已梳理的业务场景和数据处理流程进行逐一匹配。例如，对于企业的客户关系管理业务，重点关注涉及个人信息收集、存储和使用的法规；对于数据共享业务，关注数据跨境传输和第三方合作的相关规定。分析每一项法律法规对具体业务活动的影响和要求，确定哪些法律法规是适用的。在匹配过程中，识别出对企业业务影响较大、具有关键约束作用的法律法规。

将确定适用的法律法规进行整理，形成详细的数据合规法律法规清单。清单中应包括法律法规名称、相关的法律法规条款、适用声明等信息。

3. 明确数据合规管理义务

对确定适用的法律法规应进行深入解读，理解每一条款的具体含义和适用范围。法务人员可以组织内部培训或研讨会，向其他部门人员详细讲解法规内容，确保大家对法律法规要求有准确的认识。根据法律法规条款，法务人员应梳理出企业需要履行的具体合规义务。这些义务包括数据处理的合法性基础、个人信息主体权利的保障、数据安全保护措施的实施等方面。

必要时，可针对重要的合规义务编写解读文档，如个人信息主体权利保障、

数据出境合规管理等，详细说明具体要求和企业的应对措施。数据合规义务解读文档应在企业内部进行共享，为数据合规管理工作提供明确的指导和参考。

（五）评估数据合规管理风险

明确数据合规管理义务后，应结合企业当前数据管理现状评估数据合规管理风险。通过科学、系统地评估风险，企业能够提前发现潜在的合规问题，采取针对性的措施加以防范和应对，为形成合规管理共识提供重要的决策依据。如企业数据处理规模较大，建议参考 GB/T45577—2025《数据安全技术数据安全风险评估方法》进行全面的数据安全风险评估；如企业数据处理规模较小，也可以结合企业实际采用相对简单高效的评估方法，以下是评估数据合规管理风险的一般工作步骤和评估方法举例：

1. 确定风险评估范围

根据前期梳理的业务场景和数据处理流程，明确风险评估的范围。风险评估的范围一般要涵盖数据的全生命周期，包括数据收集、存储、处理、使用、共享、传输和销毁等各个环节。同时，考虑与数据相关的所有内外部因素，如企业的组织结构、业务模式、合作伙伴关系等。例如，对于电商企业，风险评估范围不仅包括平台上的用户数据处理，还应考虑与物流、支付等合作伙伴的数据交互环节。

2. 明确风险等级定义和制定风险接受准则

为了统一风险认知、支撑决策优先级和量化合规边界，避免不同部门对“高风险”的理解差异，应当明确风险等级定义和制定风险接受准则。风险接受准则

是企业基于合规义务、业务目标、风险偏好，预先设定的“可接受风险阈值”及“不可接受风险的处置规则”。它回答了：“何种风险必须规避？”（如：处理敏感个人信息未获单独同意、未匿名化的个人信息数据用于 AI 训练）；“何种风险可以容忍？”（如：内部系统临时故障导致 2 小时数据查询延迟、第三方 API 传输延迟）。

需要说明的是，风险接受准则的制定一定要遵循合规底线原则，强制符合法律法规红线。

3. 识别潜在风险点

潜在风险点可以考虑从以下几个方面进行识别：

（1）法律合规风险：对照已确定的适用法律法规与监管要求，检查企业的数据处理活动是否存在违反规定的情况。如数据收集是否获得充分的授权和同意，数据存储是否符合安全标准，数据共享是否遵循合法合规的程序等。例如，若企业在未告知用户的情况下，将用户的个人信息共享给第三方用于广告推广，就存在违反个人信息保护法规的风险。

（2）业务操作风险：分析业务流程中可能存在的风险点。如员工操作失误、内部管理不善等。例如，员工在数据录入过程中出现错误，或者未经授权的人员访问敏感数据，都可能对数据合规管理造成影响。

（3）外部合作风险：考虑与第三方合作伙伴的数据交互过程中可能产生的风险。如合作伙伴的数据保护能力不足、违反合作协议滥用数据等。例如，企业委托外部数据分析机构处理用户数据，但该机构未能采取足够的安全措施，导致数据泄露，企业可能因此承担连带责任。

（4）组织管理风险：评估企业内部的组织架构和管理机制是否有利于数据

合规管理。如是否明确了各部门的数据管理职责，是否建立了有效的沟通协调机制等。若企业内部数据管理职责不清，可能导致数据合规管理策略无法落实。

4. 评估风险发生概率和影响程度

潜在风险点的存在是否会形成重大隐患，还需要分析风险发生的可能性和影响程度：

（1）发生概率：根据企业的实际情况和历史数据，对每个潜在风险点发生的可能性进行评估。可以采用定性或定量的方法，将可能性分为高、中、低等不同的等级。例如，对于企业经常出现员工误操作的业务环节，可将其数据操作风险发生的可能性评估为“高”；对于已经采取了严格安全措施的数据存储系统，数据泄露风险发生的可能性评估为“低”。

（2）影响程度评估：分析风险一旦发生可能对企业造成的影响程度。包括对企业的法律责任、声誉、经济利益、业务运营等方面的影响。同样可以将影响程度分为高、中、低三个等级。例如，数据泄露事件若涉及大量用户的敏感个人信息，可能导致企业面临巨额罚款和声誉受损，其影响程度可评估为“高”；而一些普通业务数据的丢失，对企业业务运营影响较小，影响程度可评估为“低”。

5. 计算风险值

风险值=发生概率×影响程度。发生概率的赋值可采用历史数据统计、威胁建模、专家判断等方法，影响程度的赋值可考虑财务损失、用户影响、违法违规后果等因素。

以下举例说明风险值计算方法：

（1）赋值标准（示例）

维度	等级	定义（示例）	评分（1–5 分）
发生概率	低	年发生概率＜10%（如：数据中心断电）	1
	中	10%≤年发生概率＜30%（如：内部员工误操作）	3
	高	年发生概率≥30%（如：外部网络攻击）	5
影响程度	低	损失＜10 万元或用户投诉＜3 例（如：非敏感数据泄露）	1
	中	10 万≤损失＜500 万元或用户投诉 3–10 例（如：少量敏感业务数据泄露）	3
	高	损失≥500 万元或用户投诉＞10 例+监管调查（如：跨境传输未评估的敏感信息）	5

（2）风险矩阵（示例）

概率 影响	低（1）	中（3）	高（5）
低（1）	1（可接受）	3（中风险）	5（高风险）
中（3）	3（中风险）	9（高风险）	15（不可接受）
高（5）	5（高风险）	15（不可接受）	25（不可接受）

（3）风险等级对应（示例）

低风险：风险值≤5 分；

中风险：风险值≤6–14 分；

高风险：风险值≥15 分。

6. 制定风险应对策略

对于已经识别的风险，应进行全面的风险分析，制度风险应对策略，常见的应对策略有：

（1）风险规避：对于风险发生可能性高且影响程度严重的情况，考虑采取规避策略。例如，若某项业务活动存在较大的法律合规风险，且无法通过改进措施降低风险，企业可以考虑停止该业务活动。

（2）风险降低：针对风险发生可能性较高或影响程度较大的风险点，制定具体的措施降低风险。风险降低的具体策略可以从文化、组织、制度、技术、运

营多个维度考量，如宣传数据合规文化和组织人员意识培训、建立善数据合规管理组织和制度、加强数据安全技术措施、完善业务操作流程监督与审计等。

（3）风险转移：对于一些可以通过保险、外包等方式转移的风险，企业可以考虑将风险转移给第三方。例如，购买数据安全保险，将部分数据安全风险转移给保险公司；或者将数据处理业务外包给专业的数据处理机构，由其承担相应的风险。

（4）风险接受：对于风险发生可能性低且影响程度较小的风险点，企业可以选择接受风险，并建立监控机制，定期评估风险的变化情况。例如，对于一些偶尔发生的、对企业影响较小的系统故障风险，企业可以在做好备份和恢复准备的前提下，选择接受风险。

数据合规管理风险是动态变化的，企业应建立持续监控机制，定期对风险评估结果进行审查和更新。关注法律法规的变化、业务模式的调整、技术的发展以及外部环境的变化等因素，及时发现新的风险点或原有风险的变化情况，并相应地调整风险应对策略。例如，当新的法律法规出台对数据处理提出更高要求时，企业应重新评估相关的法律合规风险，并调整应对措施。

（六）形成数据合规管理共识

在完成了数据合规管理风险识别工作后，要尽可能与企业各个层面的人员达成数据合规管理共识，让相关人员充分的意识到数据合规管理工作对企业发展的重要影响，才能确保数据合规管理措施得到有效执行。

（1）分析合规风险与机会：风险与机会往往是并存的，数据管理与使用不善可能导致企业面临刑事诉讼、行政处罚、声誉受损、客户流失、吊销业务许可、引发高层震荡等多种风险，但同时也要意识到数据合规工作可能给企业带来的发

展机遇，如数据要素市场红利、人工智能算料支持、合规差异化竞争优势、投融资投资加分项等。

（2）明确数据合规管理目标：结合企业的实际业务情况和发展战略，确定数据合规管理的具体目标。例如，对于以在线业务为主的企业，可能目标是确保用户个人信息的安全保护，避免因数据泄露导致的法律风险和声誉损失；对于跨国企业，目标可能还包括满足不同国家和地区的数据合规要求，实现全球范围内的数据合规运营。

（3）制定数据合规管理方针和策略：方针是企业数据合规工作的方向原则，是“指南针”。策略是达成目标的执行方法，是“路线图”。应该以书面方式形成企业的数据合规管理方针和策略文件，文件内容可以包括：企业的数据合规管理目标、总体方针和原则、实现管理目标的主要策略、风险评价的准则、风险管理的基本框架、高层领导的责任及关键工作流程等。

（4）组织跨部门研讨会：组织跨部门的数据合规研讨会，让不同部门的员工共同探讨数据合规管理中存在的问题和解决方案，必要时也可请外部专家顾问参与。例如，在研讨会上，业务部门可以提出在业务开展过程中遇到的数据合规难题和业务开拓机遇，技术部门则从技术角度提供解决方案，法务和合规部门进行法律和合规层面的指导，通过这种方式促进部门间的相互理解和协作。

（5）组织培训宣贯：培训宣贯的主要内容包括但不限于数据合规相关法律法规、企业数据合规风险与机会、数据合规体系建设必要性及建设路径、网络与数据安全意识等。可以根据企业员工的不同岗位和职责，制定分层分类的培训方案。对于高层管理人员，重点培训数据合规管理的战略意义和决策层面的要求；对于业务部门员工，培训内容侧重于与业务操作紧密相关的数据合规义务和风险防范；对于技术人员，培训数据安全技术措施和合规技术要求；对于普通员工，培训网络与数据安全操作规范和安全意识。

在企业内部形成数据合规管理共识，能确保数据合规管理工作获取充分的人力、资金和资源的支持，同时也能使全体员工认识到数据合规管理的重要性，并积极参与到数据合规管理工作中，为企业的数据合规管理工作奠定文化和认知基础。

第二章 建立数据合规管理体系

本章节将探讨如何构建有效的数据合规管理体系。企业应全面收集整理现有数据合规管理相关制度文件，进行制度合规性审查，分析现有制度的优势与不足。基于分析结果和企业自身特点设计管理组织架构和组织工作机制，确保各级组织分工明确，资源配置充分，沟通协作通畅。同时，通过设计合理的制度体系结构和编制制度文件，确保各项制度之间相互协调、相互支撑，为企业的数据合规管理工作提供有力的制度保障。

（一）收集整理现有制度文件

有些企业已经建立了信息化、网络安全、数据安全以及合规管理相关的制度，甚至已经完成了一些专项建设，如 ISO/IEC 27001 信息安全管理体系认证、网络安全等级保护测评、DSMM 数据安全管理体系认证、DCMM 数据管理能力成熟度评估、PIP 个人信息保护认证、数据出境安全评估、GDPR 标准的数据隐私认证等。在建立全面的数据合规管理体系之前，对现有的管理制度进行系统梳理有助于企业了解当前管理体系的优势与不足，避免重复建设，整合资源，使新的数据合规管理制度能够更好地与现有体系相衔接。

1. 收集现有制度文件

（1）内部文件检索：在企业内部的文件管理系统、共享文件夹、各部门的资料档案中，全面检索与信息化、网络安全、数据安全、合规管理相关的制度文件。包括正式发布的规章制度、操作手册、技术规范、应急预案等。例如，信息技术部门可能保存有网络安全应急预案、信息系统运维管理办法等文件；数据管理部门可能有数据分类分级管理规定、数据备份与恢复制度等。

（2）部门沟通收集：与各部门进行沟通，确保没有遗漏重要的制度文件。有些部门可能存在尚未正式发布但实际执行的规定，通过与部门负责人和员工的交流，获取这些隐性制度信息。同时，了解各部门在执行现有制度过程中的实际操作流程和遇到的问题。

2. 分类整理制度文件

（1）按主题分类：将收集到的制度文件按照信息化、网络安全、数据安全、

合规管理等主题进行分类。在每个主题下，进一步细分具体的内容领域。例如，在网络安全主题下，可分为网络访问控制、防火墙管理、入侵检测等方面的制度；在数据安全主题下，可分为数据存储安全、数据传输安全、数据使用安全等。

（2）建立文件清单：为每一类制度文件建立详细的清单，记录文件的名称、发布部门、发布日期、主要内容概述等信息。这有助于后续对制度文件的管理和查阅，同时也能直观地了解企业在不同领域的制度建设情况。

3. 分析现有制度内容

（1）制度合规性审查：法务和合规人员对每一项制度进行深入审查，对照适用的法律法规、行业标准和监管要求，判断制度的合规性。检查制度中是否存在与法律规定相冲突的条款，是否满足最新的合规要求。例如，审查数据收集制度是否符合《个人信息保护法》中关于个人信息收集的规定。

（2）制度有效性评估：结合企业的实际业务情况和数据处理活动，评估现有制度的有效性。分析制度在实际执行中是否能够达到预期的管理目标，是否存在制度执行困难或无法落地的情况。例如，检查网络安全制度中的安全措施是否能够有效防范网络攻击，数据安全制度中的数据备份策略是否能够确保数据在意外情况下的可恢复性。

（3）制度协调性分析：审视不同主题制度之间的协调性和一致性。检查是否存在制度之间相互矛盾、重复或空白的地方。例如，信息化建设制度与网络安全制度在系统上线前的安全评估环节是否有统一的规定，数据安全制度与合规管理制度在数据违规处理流程上是否协调一致。

4. 总结现有制度的优势与不足

（1）总结优势：梳理现有制度中值得保留和发扬的部分。例如，某些制度

可能已经建立了完善的流程和机制，在实际工作中取得了良好的效果；或者一些制度体现了企业在特定领域的先进管理理念和技术手段。将这些优势总结出来，以便在新的数据合规管理制度中继续应用和强化。

（2）识别不足：明确现有制度存在的问题和不足之处。可能包括制度内容过时、不符合最新法规要求、执行难度大、缺乏有效的监督和考核机制等。对这些不足进行详细记录和分析，为后续设计制度体系架构和编写新制度提供改进方向。

（二）设计数据合规管理组织架构

科学合理的组织架构将为后续的管理制度编制以及组织的有效运行提供重要指引，确保数据合规管理体系能够切实落地并发挥作用。以下是设计数据合规管理组织架构的具体工作步骤：

1. 分析企业自身特点与需求

在搭建数据合规管理的组织架构时，企业应充分考虑自身的业务、数据资源及人力资源等情况，结合企业自身特点与需求设计有针对性的、符合企业运作机制的管理组织。

（1）评估企业规模与业务复杂性：对企业的规模进行全面评估，包括员工数量、业务范围、市场覆盖区域等方面。同时，分析企业业务的复杂性，如业务流程的繁琐程度、数据处理的多样性等。例如，大型企业可能需要更复杂、多层次的组织架构来应对庞大的数据管理工作；而小型企业则可以采用相对简洁的架构，以提高管理效率。业务复杂的企业可能需要设置专门的部门或岗位来处理特定的数据合规问题，如数据跨境传输管理等。

（2）考虑企业数据资产状况：分析企业的数据资产，包括数据的类型（如个人信息、商业机密、业务运营数据等）、数量、价值以及数据的产生、存储、使用和流转情况。根据数据资产的特点，确定组织架构中对数据管理的重点和方向。例如，对于拥有大量高价值用户个人信息的数据资产的企业，组织架构应侧重于加强个人信息保护的相关职能。

（3）结合企业现有管理模式：分析企业现有的管理模式和组织文化，考虑如何将数据合规管理组织融入其中。如果企业采用扁平化管理模式，数据合规管理组织的架构设计可以相对灵活，强调部门之间的协作和沟通；如果企业具有层级分明的管理模式，则组织架构可以与之相适应，明确各层级的职责和权限。

2. 确定组织架构设计的原则

企业数据合规管理组织架构的设计要考虑法规适配性、协同性、实际运行的适应与高效性多方面因素，具体原则包括：

（1）合规性原则：确保组织架构的设计严格遵循国内外与数据相关的法律法规和行业监管要求。如依据《个人信息保护法》第五十二条的规定，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。

（2）协同性原则：强调组织内部各部门之间的协同合作。数据合规管理工作涉及多个部门，如法务、技术、业务等，需要各部门之间密切配合。在组织架构设计中，明确各部门在数据合规管理中的职责和协作流程，建立有效的沟通机制。例如，在数据安全事件处理过程中，信息技术部门负责技术层面的应急响应，法务部门提供法律支持，合规管理部门进行监督和协调，共同应对事件。

（3）适应性原则：组织架构应具有一定的灵活性和适应性，能够随着企业业务的发展、法律法规的变化以及技术的进步而进行调整。预留一定的弹性空间，

以便在需要时能够及时增设或调整部门和岗位。当企业拓展新的业务领域或进入新的市场时，组织架构能够迅速适应新的合规要求。

（4）效率性原则：在保证数据合规管理工作有效开展的前提下，追求组织架构的高效运行。避免架构过于复杂导致的管理成本增加和效率低下。合理设置部门和岗位，明确职责分工，减少不必要的流程和环节。也可以考虑通过信息化手段实现数据的自动化管理和合规监控，提高工作效率。

3. 规划组织架构层级和职责

一个良好的数据合规管理团队，通常由决策层、管理层、执行层和监督层四个层面组成，企业需要明确各层面的职责、涉及的人员及对应的岗位。各层面的主要职责如下：

（1）决策层

决策层是数据合规管理的决策机构，对数据合规管理负领导责任。为保证公司在数据合规方面的决策能够落实，决策层宜由公司内部职级高、拥有跨部门统筹协调工作的高级管理人员组成。企业可根据实际情况，由董事长或执行董事、法定代表人、CTO、CIO、CDO 组建数据合规管理委员会等来组成决策层。决策层主要负责如下事务：

①为企业数据合规管理制度体系的建构和运行提供必要的资源保障和条件支持，确保合规管理制度体系有效运转并持续改进；

②确立数据合规的愿景、目标和战略，并确保数据合规管理战略与企业战略方向保持一致；

③保障数据合规管理部门具备独立履行职责的能力与权限；

④审批企业重大数据合规事项；

⑤确保将数据合规管理要求融入企业的业务开展过程；

⑥确保建立有效的数据违规举报与惩处机制；

⑦引导培育企业数据合规自主性，促成数据合规企业文化；

⑧其他与数据合规领导决策相关工作。

（2）管理层

管理层是数据合规管理的管理机构，实际承担数据合规管理的日常管理工作，企业应设立专门的数据合规管理部门，或者可以由合规部门、法务部门、安全部门等部门承担数据安全管理职责，但需要配备数据合规专员。管理层主要负责如下事务：

①组织制定企业数据合规管理制度规范与合规计划，并推动其有效实施；

②统筹实施数据合规管理工作，并对数据合规管理情况进行评估与检查；

③建立数据合规举报与调查机制，对数据合规举报制定调查方案并开展调查；

④定期组织或协助人事部门开展数据合规培训，为企业相关内部职能部门提供数据合规咨询与支持；

⑤向决策层报告数据合规重大风险和数据合规工作落实情况；

⑥其他与数据合规日常管理相关的工作。

（3）执行层

执行层由企业内部涉及数据处理工作的所有职能部门组成，执行层主要职责如下：

①结合企业数据合规管理制度和合规指引，明确本部门日常数据处理活动的全生命周期合规要求和具体工作机制；

②确保本部门员工遵守企业合规制度规范，履行数据合规义务；

③配合数据合规管理负责人和合规管理部门开展合规风险审查、评估、整改等各项合规工作；

④密切监测日常数据处理工作中的数据合规风险，并采取适当的安全保护措施；

⑤当发现数据处理活动存在较大合规风险或者发生数据安全事件时，及时向数据合规管理负责人和合规管理部门报告，并配合采取应急处置和整改措施；

⑥其他与数据合规具体执行相关的工作。

（4）监督层

监督层独立于决策层、管理层、执行层，监督层与决策层、管理层、执行层人员不得有交叉，避免对监督层独立履行职责产生干扰。监督层主要履行对企业数据合规管理工作开展情况的监督职责，主要负责如下事项：

①负责对决策层针对数据合规管理事项做出的决策进行监督，确保相关决策过程符合法律法规及企业规章制度的规定；

②负责对管理层制定的制度规范、合规计划及日常管理工作等进行监督，确保相关管理工作开展符合法律法规及企业规章制度，且与企业的数据合规管理战略保持一致；

③负责对执行层落实数据合规管理各项制度及工作安排情况进行监督；

④定期对企业数据合规管理工作开展审计；

⑤参与考核评价工作，在考核过程中如实提出监督过程中发现的问题；

⑥其他与数据合规监督管理相关的工作。

4. 建立沟通和协作机制

建立健全的沟通和协作机制不仅能够确保信息流通顺畅、提升工作效率和增强团队凝聚力，还能够促进知识共享和学习、及时应对突发事件和合规风险。以下是建立沟通和协作机制的具体工作步骤：

（1）分析信息流动：分析数据合规管理工作中信息在各层级之间的流动情况，包括决策信息的传达、执行情况的反馈、问题和风险的报告等。确定信息传递的关键节点和渠道，评估现有沟通方式的有效性。例如，是否存在信息在传递

过程中失真或延误的情况，是否有合适的平台或机制确保信息的及时共享。对于监督层，要特别明确其发现问题后信息上报的流程和接收对象，保证监督信息能够准确、迅速地传达。

（2）确定沟通和协作机制：根据各层级的职责和工作流程，确定层级间的协作机制。例如，建立定期的沟通会议制度，让管理层向决策层汇报工作进展和问题，执行层向管理层反馈执行情况，监督层通报监督结果；设立跨层级的项目小组，共同处理复杂的合规问题；明确在紧急情况下的协作流程和责任分工，确保能够迅速应对突发的合规事件。同时，建立监督层与其他层级之间的协作机制，如监督层在审计和巡查过程中需要其他层级配合提供资料和信息时的协作流程。

5. 建立监督和评价机制

建立健全的监督和评价机制是确保组织有效运行、数据合规管理目标得以实现的保障。监督和评价机制能够及时发现数据合规管理工作中的问题与不足，为改进和优化管理措施提供依据。以下是建立监督评和价机制的具体工作步骤：

（1）确定监督和评价目标：组织相关人员共同研讨，明确监督和评价机制的目标。其核心目标是确保企业的数据处理活动符合国内外法律法规、行业标准以及企业内部的数据合规管理制度，保护数据主体的合法权益，降低数据合规风险。例如，通过监督确保企业在数据收集环节获得数据主体的有效同意，通过评价促进数据安全技术措施的持续改进。

（2）界定监督和评价范围：全面梳理数据合规管理的各个环节，确定监督和评价的范围。涵盖数据的全生命周期，包括数据收集、存储、处理、使用、共享、传输和销毁等活动；涉及企业内部的各个部门和岗位，无论是业务部门、技术部门还是管理部门，都在监督和评价的范畴之内；同时，还应包括对数据合规管理体系的整体有效性、合规文化的建设情况等方面的评估。

（3）制定监督标准：依据适用的法律法规、行业标准以及企业内部的数据合规管理制度，制定具体的监督标准。例如，在数据收集方面，标准可以包括收集目的的明确性、收集方式的合法性、数据主体同意的有效性等；在数据存储方面，标准涵盖数据存储的安全性、存储期限的合规性等。确保监督标准具有可操作性和可衡量性，为监督工作提供明确的依据。

（4）选择监督方法：采用多种监督方法，如文件审查、现场检查、数据抽样分析、员工访谈等。文件审查主要针对数据处理相关的合同、协议、政策文件等，检查其合规性；现场检查可以实地查看数据处理设施、操作流程等，发现实际工作中的问题；数据抽样分析通过抽取一定数量的数据样本，检查数据的准确性、完整性和合规性；员工访谈则了解员工对数据合规制度的理解和执行情况。

（5）确定评价指标：建立一套科学合理的评价指标体系，用于衡量数据合规管理工作的成效。指标可以包括合规制度的完善程度、合规培训的覆盖率、数据安全事件的发生率、监管机构的处罚次数等。根据不同的评价指标，设定相应的权重，以便综合评估数据合规管理工作的整体水平。

（6）选择评价方法：运用定性和定量相结合的评价方法。定性评价主要通过对合规管理工作的整体情况进行分析和判断，如评估合规文化的建设氛围、员工的合规意识等；定量评价则依据具体的数据和指标进行计算和分析，如计算数据安全事件的发生率、合规培训的参与率等。通过综合运用定性和定量评价方法，得出客观、准确的评价结果。

（三）设计数据合规管理体系架构

合理的制度体系架构能够确保各项制度之间相互协调、相互支撑，为企业的数据合规管理工作提供有力的制度保障。以下是设计制度体系架构的具体工作步骤：

1. 确定管理体系文件的层级

（1）基本制度：应该以书面方式形成企业的数据合规管理方针和策略文件，文件内容可以包括：企业的数据合规管理目标、总体方针和原则、实现管理目标的主要策略、风险评价的准则、风险管理的基本框架、高层领导的责任及关键工作流程等。

（2）具体规定：根据数据处理的不同环节和业务领域，明确具体的管理规定。这些制度应详细规定数据收集、存储、处理、使用、共享、传输和销毁等环节的具体规则和要求。例如，数据收集制度应明确收集的目的、方式、范围、程序以及同意的获取方式等。

（3）操作细则：针对具体制度，制定详细的操作细则，明确各项工作的具体操作流程、方法和标准。例如，在数据访问控制操作细则中，明确用户权限的分配、审批和管理流程。

（4）记录表单：针对制度执行情况，应做好可溯源的过程记录，这些记录文件应该是规范统一的。例如任命记录、培训记录、检查记录、审计记录、事件处置记录、评估记录、各类清单和评价表等。

2. 明确制度之间的关系和衔接

（1）梳理制度间的逻辑关系：分析各项制度之间的逻辑关系，确保制度体系的一致性和协调性。例如，数据收集制度是数据使用和共享制度的前提，数据安全制度贯穿于数据生命周期的各个环节，为其他制度的实施提供保障。

（2）建立制度衔接机制：制定制度之间的衔接机制，避免出现制度冲突或空白。例如，在数据处理流程中，当数据从收集环节进入存储环节时，应明确数据的交接方式、质量标准和安全责任；在数据共享过程中，涉及多个制度的协同

执行，应建立相应的协调机制。

（3）确保制度的可追溯性：设计制度体系时，要考虑制度的可追溯性，便于对数据处理活动进行审计和监督。通过建立数据记录、日志管理等机制，能够追踪数据的来源、处理过程和流向，为合规审查和问题追溯提供依据。

龙华区某企业数据合规管理体系文件举例：

文件级别	文件类型	文件名称
一级文件	纲领性文件，按方针目标和适用的标准综合描述组织管理体系总体要求	数据合规管理总体方针和策略
二级文件	管理规定性文件，描述管理要素及具体要求	数据合规组织管理规定、数据分类分级管理规定、数据全生命周期管理规定、数据跨境传输管理规定、数据合作方管理规定、数据安全培训宣贯规定、数据安全风险评估规定、个人信息保护影响评估管理规定、数据合规审计管理规定、个人信息主体权利响应和投诉举报管理规定、数据安全事件管理规定、监管执法配合工作规定
三级文件	操作规范性文件，描述具体操作流程和方法细节	数据访问控制操作细则、个人信息保护影响评估操作指引、数据安全事件应急预案、个人信息保护政策模板、数据合作方合规尽职调查问卷模板、数据出境操作指引、个人信息保护投诉和举报操作指引、员工手册
四级文件	记录表单文件，用于表明结果和记录过程，具备溯源功能	任命记录、培训记录、检查记录、审计记录、事件处置记录、评估记录、各类清单和评价表等

（四）编写数据合规管理制度文件

编写数据合规管理制度需要综合考虑企业的实际情况、法律法规要求以及数据合规管理的目标，确保制度的全面性、适用性和有效性。以下是常见的数据合规管理制度及编写要点：

数据合规管理总体方针和策略	
编写目的	明确数据合规管理目标、总体方针和原则、实现管理目标的主要策略等基本要求。
编写要点	方针是企业数据合规工作的方向原则，是“指南针”。策略是达成目标的执行方法，是“路线图”。应该以书面方式形成企业的数据合规管理方针和策略文件，文件内容可以包括：企业的数据合规管理目标、总体方针和原则、实现管理目标的主要策略、风险评价的准则、风险管理的基本框架、高层领导的责任及关键工作流程等。
数据合规组织管理规定	
编写目的	明确组织架构、职责分工、组织管理机制。
编写要点	1.设立数据合规管理各级组织，定义其职责； 2.确定数据合规管理岗位角色的职责、权限及任职要求； 3.明确各业务部门的数据合规责任； 4.规定合规承诺、举报调查、沟通协作、考核评价、人员培训、离岗审计等相关要求。
数据分类分级管理规定	
编写目的	依据国家法律法规和标准规范明确数据分类分级原则和方法，并规定不同级别的保护措施。

编写要点	1.数据分类分级依据； 2.数据分类分级原则和标准； 3.数据分类分级方法； 4.不同级别数据的处理、存储、访问权限要求； 5.定期复审与调整机制。
数据全生命周期管理规定	
编写目的	覆盖数据从收集到删除的全过程管理要求。
编写要点	1.企业数据处理活动应遵循合法、正当、必要、诚信原则，不得非法收集和处理数据； 2.数据传输应采用安全协议，确保数据在传输过程中的安全； 3.数据存储应采取加密、脱敏等安全措施，确保数据在存储过程中的安全，对不同类型的数据采取不同的存储策略； 4.数据使用管理应遵循最小化原则，访问数据需要基于身份执行授权、访问控制、审计机制； 5.数据加工、委托处理、提供、公开前，应进行风险评估，确保数据安全； 6.数据销毁应遵循合法合规、安全原则，确保数据无法恢复； 7.涉及处理重要数据、敏感个人信息、对外提供、委托、公开、自动化决策等情况的，企业应留存处理记录，至少三年。
数据跨境传输管理规定	
编写目的	确保跨境数据传输符合法律法规要求。
编写要点	1.数据出境前，企业需要先进行安全自评估，涉及个人信息出境的，需要做个人信息保护影响评估； 2.企业应建立数据出境的审批流程，明确审批的层级、权限和责任； 3.企业应根据法律法规的规定及安全自评估情况，识别并选择合适的数据出境路径，如申报数据出境安全评估、签订个人信息出

	境标准合同并备案、通过个人信息保护认证或直接出境； 4.企业应应对数据出境进行定期审查和风险评估，及时发现和处置潜在的安全风险； 5.企业应建立数据出境用户权益保障机制，明确在数据出境过程中以及用户权益受到侵犯时，用户行使其权利的途径、方式等； 6.留存向境外提供数据的记录，至少三年。
数据合作方管理规定	
编写目的	确保与合作方在数据处理和共享过程中的安全性和合规性。
编写要点	1.企业应明确合作方的选择标准和流程，包括资质审查、业务审查、事项审批等； 2.通过协议、合作方管理规范等文件，明确合作方在数据安全方面的责任和义务； 3.针对合作方人员访问企业数据资源的情况，应建立覆盖权限申请、审批、变更、注销的全生命周期管理制度； 4.对数据合作方的数据操作行为进行日志留存，包括人员、操作数据类型、操作行为、操作时间等； 5.定期对合作方的数据使用行为进行审计，包括认证记录、访问记录、操作记录等。用以发现异常操作、敏感数据操作等，并留存审计记录； 6.对合作方使用数据的权限和范围进行限制，确保数据不被滥用或泄露。
数据安全培训宣贯规定	
编写目的	提升全员数据安全意识与技能。
编写要点	1.企业应明确数据安全培训的目标，如提高员工的数据安全意识、掌握数据安全的基本知识和技能、了解数据安全法律法规等，以确保企业数据资产的安全； 2.确定数据安全培训的对象，通常包括企业全体员工，特别是 IT

	人员、财务人员、人力资源人员等关键岗位的员工； 3.培训内容可以包括但不限于：数据安全基本概念、数据合规管理制度、数据安全技术、据安全事件应对、数据安全法律法规等； 4.培训方式可以包括但不限于：讲解与讨论、案例分析、实践操作等。
个人信息保护影响评估管理规定	
编写目的	依据个人信息保护法相关法律法规要求，规范企业个人信息保护影响评估工作，保护个人信息权益。
编写要点	1.有下列情形之一的，企业应当事前进行个人信息保护影响评估，并对处理情况进行记录： ①处理敏感个人信息； ②利用个人信息进行自动化决策； ③委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息； ④向境外提供个人信息； ⑤其他对个人权益有重大影响的个人信息处理活动。 2.个人信息保护影响评估评估内容、评估流程可结合业务实际和法律法规要求，参考 GB/T 39335-2020《信息安全技术个人信息安全影响评估指南》制定; 3.个人信息保护影响评估报告和处理情况记录的保存期限，一般应至少保存三年； 4.企业应明确内部各部门和人员在个人信息保护影响评估工作中的职责，对于未按照规定履行职责，导致个人信息泄露或其他安全事件发生的，依法追究相关人员的责任。
数据安全风险评估规定	
编写目的	定期识别、评估数据安全风险，制定应对措施，确保数据处于有效保护和合法使用的状态。

编写要点	1.企业应明确数据安全风险评估的目的、范围和原则； 2.风险评估的内容可包括数据处理活动合规性、安全管理制度与措施、组织与人员管理、技术防护能力等； 3.重要数据和核心数据处理者每年至少开展一次评估。在有效期内出现如新增跨主体提供、委托处理、转移核心数据；重要数据、核心数据安全状态发生变化对数据安全造成不利影响；发生涉及重要数据、核心数据的安全事件等情形时，应当及时对发生变化及其影响的部分开展风险评估； 4.明确评估报告的审核流程，以及向内部相关部门、管理层和外部监管机构报送的要求； 5.根据评估结果制定针对性的数据安全防护策略，包括技术防护措施和管理措施； 6.明确企业内部各部门、人员在数据安全风险评估工作中的职责，以及在数据安全事件中的责任追究机制。
数据合规审计管理规定	
编写目的	通过合规审计及时发现问题并进行整改，确保数据合规管理体系有效运行。
编写要点	1.企业应明确数据合规审计工作流程、方法、审计触发条件及审计结果运用相关规定； 2.审计流程包括审计计划、审计准备、审计实施、审计报告、审计整改等阶段； 3.审计方法包括现场审计、远程审计、问卷调查、访谈等多种方法相结合； 4.审计结果应作为企业改进数据合规管理的重要依据，用于指导企业完善数据安全防护措施、加强数据合规培训和宣传等工作； 5.企业应建立健全数据合规审计监督机制，对审计过程进行全程监督，确保审计工作的规范性和有效性； 6.对于在合规审计中发现的问题和违规行为，企业应依法依规进行责任追究，严肃处理相关责任人； 7.处理超过 1000 万人个人信息的个人信息处理者，应当应当自行

	或者委托专业机构每两年至少开展一次个人信息保护合规审计； 8.涉及未成年人个人信息处理的，应当自行或者委托专业机构每年对其处理未成人个人信息遵守法律、行政法规的情况进行合规审计，并将审计情况及时报告网信等部门。
个人信息主体权利响应和投诉举报管理规定	
编写目的	规范个人信息主体权利响应和投诉举报的管理流程，确保个人信息主体合法诉求得到及时、公正、有效的处理。
编写要点	1.当用户向个人信息处理者行使其个人信息权利时，企业有义务给出合理、便捷的行权入口、行权路径以及响应方式，并且需要在合理期限内进行响应； 2.面向公共服务的个人信息处理业务应建立用户个人信息保护举报投诉渠道，明确举报投诉处理部门和人员、处理流程、处理要求等。针对有效举报线索，及时核查处理并在接到投诉之日起十五日内答复投诉人； 3.企业应设立多种投诉举报渠道，包括但不限于电话、邮件、官方网站、微信公众号、现场投诉等，确保用户能够方便快捷地提出投诉举报；投诉举报人可以通过上述渠道，以文字、图片、视频等形式提出投诉举报，并应提供尽可能详细的信息，包括投诉举报的具体内容、时间、地点、涉及人员等； 4.企业应设立专门的投诉举报受理机构或岗位，负责接收、登记、审查投诉举报信息，确保信息得到及时、准确的记录和处理；投诉举报受理后，企业应按照规定的流程和时间要求对投诉举报进行调查核实，收集相关证据，形成调查报告，并根据调查结果采取相应的处理措施。处理措施应包括但不限于纠正违规行为、给予责任人处罚、加强数据合规培训等； 5.企业应对投诉举报人的个人信息和投诉举报内容进行保密，防止信息泄露和滥用；企业不得对投诉举报人进行打击报复或恶意陷害。

数据安全事件管理规定	
编写目的	建立健全数据安全事件的预防、发现、报告、处置和恢复机制，提高数据事件处理的及时性和有效性。
编写要点	1.企业应建立数据安全事件管理组织机构，并明确其职责； 2.参考《信息安全技术信息安全事件分类分级指南》等标准，结合企业实际，将数据安全事件进行分类分级； 3.明确通过何种技术手段和管理措施对数据安全进行监测，规定预警的发布流程和方式； 4.明确发现数据安全事件后，员工应如何报告，报告的渠道、时间要求、报告内容等； 5.针对不同类型和级别的数据安全事件，制定具体的处置措施； 6.定期组织数据安全事件应急演练，模拟不同类型和级别的数据安全事件，检验和评估应急响应机制的有效性； 7.对于在数据安全事件中存在失职、渎职行为，或违反制度导致事件发生的人员，明确相应的责任追究机制和处罚措施； 8.定期对数据安全事件管理制度进行审查和改进，以适应不断变化的数据安全环境。
监管执法配合工作规定	
编写目的	通过制定数据合规监管执法配合工作制度，明确企业在应对司法或者执法机构工作时的配合流程、责任分工和具体要求，确保配合工作高效、有序进行。

编写要点	1.企业应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助； 2.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； 3.履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施： ①询问有关当事人，调查与个人信息处理活动有关的情况; ②查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料; ③实施现场检查，对涉嫌违法的个人信息处理活动进行调查; ④检查与个人信息处理活动有关的设备、物品;对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。企业应当予以协助、配合，不得拒绝、阻挠； 4.履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。企业应当按照要求采取措施，进行整改，消除隐患； 5.企业应明确监管执法配合工作相关部门责任分工，确保各部门之间的顺畅沟通和协作。

（五）组织管理制度发布与宣贯

完成制度初稿编写后，应组织制度评审工作。评审人员可以包括企业内部的法务、合规、技术、业务等相关部门人员，也可以包括外部专家。评审内容可包括制度的合法性、全面性、适用性、有效性以及与企业实际情况的契合度等。评审通过后，应通过规范的发布流程和全面的宣贯活动，使企业全体员工了解、熟悉并遵守制度，将数据合规管理理念融入到日常工作中。

1. 组织内部评审

通过发放调查问卷、组织评审会等方式，广泛收集企业各部门对制度的意见和建议。对收集到的意见和建议进行分类整理，对制度中存在的法律问题、操作难题、逻辑矛盾等进行修改和完善。

2. 组织专家评审

在组织内部评审的基础上，还可以考虑邀请外部专家参与制度评审。组织专家评审是进一步提升制度质量、确保其科学性和有效性的重要手段。通过邀请专业领域的专家对制度进行全面评估，可以发现潜在的问题和不足，借助专家的经验和专业知识对制度进行优化，使其更符合法律法规要求、行业最佳实践以及企业实际情况。

3. 制度发布与宣贯

在完成数据合规管理制度的编写、专家评审以及修订工作后，应通过规范的发布流程和全面的宣贯活动，使企业全体员工了解、熟悉并遵守制度，将数据合规管理理念融入到日常工作中。以下是制度发布与宣贯的具体工作建议：

（1）确定发布形式与范围

根据企业的实际情况和员工的工作特点，选择合适的制度发布形式。常见的发布形式包括企业内部正式文件发布、内部网站公告、电子邮件通知、印刷成册发放等。制度的发布范围应确保所有涉及数据处理活动的部门、岗位和人员都能获取到制度内容。不仅包括直接参与数据处理的业务部门、技术部门，还应涵盖管理部门、后勤部门等可能接触到数据的相关人员。对于企业的分支机构、子公

司等，也需要将制度及时传达，确保整个企业体系内的数据合规管理标准一致。

（2）正式发布制度

按照企业内部的文件发布程序，办理相关审批手续。由企业高层领导或相关负责人对制度进行审批签字，确保制度的权威性和严肃性。审批通过后，按照预定的发布形式和范围，将制度正式发布。在发布过程中，记录发布的时间、方式、范围等信息，以便后续进行跟踪和管理。

（3）组织制度宣贯

根据企业的规模、员工分布、工作特点等因素，选择合适的宣贯方式。常见的宣贯方式包括集中培训、线上学习、内部刊物宣传、海报展示、知识竞赛等。对于规模较大、员工分布较广的企业，可以采用线上学习与集中培训相结合的方式；对于一些简单易懂的制度内容，可以通过内部刊物、海报等形式进行宣传。此外，还可以组织知识竞赛等活动，激发员工的学习积极性和参与热情。

第三章 完善数据安全技术措施

本章节将分析如何分步骤完善数据安全技术措施。通过检查企业数据处理的基础设施和网络系统，评估数据全生命周期技术控制措施，清晰掌握数据安全技术现状。依据评估结果，结合企业业务需求和发展战略，制定出贴合实际的、具有前瞻性的数据安全策略与方案。按照规划有序部署各类数据安全技术，逐步形成完善的数据安全技术体系，支撑数据合规管理体系的有效落地。

（一）评估现有数据安全技术状况

企业可以在第一阶段数据合规管理风险评估的基础上，进一步评估现有数据安全技术状况，发现企业在数据安全技术方面存在的问题与漏洞，为后续制定针对性的数据安全建设规划方案提供有力依据。以下是评估现有数据安全技术状况的具体工作步骤：

1. 检查基础设施

（1）检查数据处理设备：对企业的数据处理设备（如硬盘阵列、服务器、云存储等）进行检查。查看设备的性能指标，如存储容量、读写速度、可靠性等是否满足业务需求；检查存储设备的安全配置，如是否启用了数据加密、访问控制等功能；评估存储设备的备份和恢复机制是否健全，能否在数据丢失或损坏时及时恢复数据。

（2）审查网络系统：依据国家网络安全等级保护要求相关标准审查企业的网络系统，包括网络拓扑结构、网络设备（路由器、交换机、防火墙等）的配置和运行状态。检查网络拓扑是否合理，是否存在单点故障风险；评估入侵防御的规则设置是否有效，能否抵御外部网络攻击；检查网络设备的软件版本是否及时更新，以防止因软件漏洞导致的安全问题。

2. 开展安全漏洞检测

（1）使用专业检测工具：运用专业的安全检测工具，如漏洞扫描器、自动化渗透测试工具、API 接口安全检测等，对企业的数据系统和网络进行全面检测。

漏洞扫描器可以快速发现系统中存在的已知漏洞，如操作系统漏洞、数据库漏洞、应用程序漏洞等；渗透测试工具则通过模拟黑客攻击的方式，评估系统的安全性和防护能力，发现潜在的安全风险；API 接口安全检测工具可以全面梳理企业数据接口资产信息，识别潜在数据交互风险。

（2）进行人工安全评估：除了使用工具检测外，评估团队还应进行人工安全评估。通过对系统的配置文件、日志记录等进行分析，发现一些工具无法检测到的安全问题，如安全策略的不合理配置、潜在的内部安全威胁等。

3. 审查数据全生命周期安全技术措施

（1）数据收集阶段：审查数据收集工具和系统是否具备合法获取数据的技术手段，例如是否能够准确记录数据来源、获取时间等信息。评估数据收集过程中的身份验证和授权技术，确保只有授权主体才能进行数据收集操作，防止非法采集。检查数据收集系统是否具备数据验证功能，以保证收集到的数据的准确性和完整性。

（2）数据传输阶段：评估数据在内部网络和外部网络传输时所采用的加密技术，如 SSL/TLS 协议等，确保数据在传输过程中不被窃取、篡改或监听。审查数据传输过程中的访问控制技术，对传输通道进行权限管理，防止未授权的访问和数据泄露。检查数据传输监控和审计技术，能够实时监测数据传输状态，记录传输日志，以便在出现问题时进行追溯和分析。对于跨境数据传输，评估是否具备相应的技术措施来满足法规要求，如数据出境安全评估相关的技术保障等。

（3）数据存储阶段：检查数据存储系统的访问控制技术，如多因素认证、权限分级管理等，确保只有授权人员能够访问存储的数据。评估数据加密技术，包括存储加密算法的强度、密钥管理的安全性等，防止数据在存储过程中被窃取

或泄露。查看数据备份和恢复技术的可靠性，确保在数据丢失或损坏时能够及时恢复数据，同时检查备份数据的存储安全。

（4）数据处理阶段：审查数据访问和使用的审计技术，是否能够详细记录数据的访问时间、访问人员、操作内容等信息，以便进行合规审计。评估数据脱敏和匿名化技术，确保在数据使用过程中对敏感信息进行有效保护，防止数据滥用。检查数据使用过程中的权限动态管理技术，能够根据业务需求和人员角色变化及时调整数据访问权限。

（5）数据交换阶段：评估数据交换平台的安全防护技术，如数据传输加密、访问控制、安全审计等，确保数据在交换过程中的安全性。检查数据交换过程中的数据溯源技术，能够追踪数据的流向和使用情况，防止数据被非法共享或泄露。审查数据交换的授权管理技术，确保数据交换是基于合法的授权和审批流程。

（6）数据销毁阶段：检查数据销毁工具和技术的有效性，如数据擦除算法是否能够彻底清除数据，确保数据无法恢复。评估数据销毁过程的记录和审计技术，能够提供完整的数据销毁记录，以证明数据已被合法销毁。

4. 评估数据安全技术能力

评估数据安全技术能力可参考 GB/T37988-2019《信息安全技术数据安全能力成熟度模型》。企业可通过该标准评估当前数据处理活动的每个环节的安全技术能力级别，并结合自身业务特点和合规建设需求确定期望建设达到的级别。

（1）数据收集安全技术能力

数据收集安全技术能力包括了数据分类分级、数据源鉴别及记录、数据质量管理等方面的能力。以下是对数据收集安全技术能力不同级别的特征描述：

级别	特征描述
1 级	无
2 级	核心业务具有技术工具支持对数据源的鉴别和记录
3 级	1）建立数据分类分级打标或数据资产管理工具，实现对数据的分类分级自动标识、标识结果发布、审核等功能； 2）依据统一的数据采集流程建设数据采集相关的工具，以保证组织数据采集流程实现的一致性，同时相关系统应具备详细的日志记录功能，确保数据采集授权过程的完整记录； 3)采取技术手段保证数据采集过程中个人信息和重要数据不被泄漏； 4）采取技术手段对外部收集的数据和数据源进行识别和记录； 5）对关键追溯数据进行备份，并采取技术手段对追溯数据进行安全保护； 6）应利用技术工具实现对关键数据进行数据质量管理和监控，实现异常数据及时告警或更正。
4 级	1）应记录自动分类分级结果与人工审核后的分类分级结果之间的差异，定期分析改进分类分级标识工具，提升工具处理的准确度； 2）对数据分类分级的操作、变更过程进行日志记录和分析，定期通过日志分析等技术手段进行变更操作审计，数据分类分级可追溯； 3）关键的数据管理系统中提供了标记数据的数据源类型的功能，从而实现对组织内部各类数据源的统计和分析。
5 级	1)跟踪数据分类分级标识效果，持续改进数据分类分级的技术工具； 2)面向制度流程的更新，持续改进工具在数据鉴别、记录和追溯等方面的服务能力；

	3)建立数据质量的技术指标，并通过相关管理系统评估数据质量管理的水平； 4)参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆。

（2）数据传输安全技术能力

数据传输安全技术能力包括了数据传输加密、网络可用性管理等方面的能力。以下是对数据传输安全技术能力不同级别的特征描述：

级别	特征描述
1 级	无
2 级	1）有对传输通道两端进行主体身份鉴别和认证的技术方案和工具； 2）有对传输数据加密的技术方案和工具，包括针对关键的数据传输通道的加密方案(如采用 TLS/SSL 方式)，及对传输数据内容进行加密。
3 级	1）有对传输数据的完整性进行检测，并具备数据容错或恢复的技术手段； 2）部署对通道安全配置、密码算法配置、密钥管理等保护措施进行审核及监控的技术工具应对关键的网络传输链路、网络设备节点实行冗余建设； 3)）部署相关设备对网络可用性及数据泄漏风险进行防范，如负载均衡、防入侵攻击、数据防泄漏检测与防护等设备。
4 级	1）每个传输链路上的节点都应部署了独立密钥对和数字证书，以保证各节点有效的身份鉴别； 2）综合量化敏感数据加密和数据传输通道加密的实现效果和成本，定

	期审核并调整数据加密的实现方案； 3）提供统一的数据加密模块供开发传输功能的人员调用，根据不同数据类型和级别进行数据加密处理，保证组织内数据加密功能的统一性； 4）通过相关指标定量分析网络可用性及数据防泄漏服务现状，并有针对性地解决问题，提升网络可用性。
5级	1）跟进传输通道加密保护的技术发展，评估新技术对安全方案的影响，适当引入新技术以应对最新的安全风险； 2）实现网络安全设备的健康状态检查及自动化切换； 3）参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆。

（3）数据存储安全技术能力

数据存储安全技术能力包括了存储媒体安全、逻辑存储安全、数据备份和恢复等方面的能力。以下是对数据存储安全技术能力不同级别的特征描述：

级别	特征描述
1级	无
2级	1）采取技术工具支撑逻辑存储系统的安全管理，如配置扫描、身份鉴别、访问控制等； 2）建立数据备份与恢复的技术工具。
3级	1）使用技术工具对存储媒体性能进行监控，包括存储媒体的使用历史、性能指标、错误或损坏情况，对超过安全阈值的存储媒体进行预警； 2）对存储媒体访问和使用行为进行记录和审计； 3）提供数据存储系统配置扫描工具，定期对主要数据存储系统的安全配置进行扫描，以保证符合安全基线要求；

	4）利用技术工具监测逻辑存储系统的数据使用规范性，确保数据存储符合组织的相关安全要求； 5）具备对个人信息、重要数据等敏感数据的加密存储能力； 6）建立数据备份与恢复的统一技术工具，保证相关工作的自动执行； 7）建立备份和归档数据安全的技术手段，包括但不限于对备份和归档数据的访问控制、压缩或加密管理、完整性和可用性管理，确保对备份和归档数据的安全性、存储空间的有效利用、安全存储和安全访问； 8）定期采取必要的技术措施查验备份和归档数据完整性和可用性； 9）建立过期存储数据及其备份数据彻底删除或匿名化的方法和机制，能够验证数据已被完全删除、无法恢复或无法识别到个人，并告知数据控制者和数据使用者； 10）通过风险提示和技术手段避免非过期数据的误删除，确保在一定的时间窗口内的误删除数据可以手动恢复； 11）确保存储架构具备数据存储跨机柜或跨机房容错部署能力。
4级	1）建立存储媒体管理系统，确保存储媒体的使用和传递过程得到严密跟踪； 2）建立管理数据存储系统安全配置的技术工具，实现对安全配置情况的统一管理和控制； 3）建立可伸缩数据存储架构，以满足数据量持续增长、数据分类分级存储等需求； 4）建立满足应用层、数据层、操作系统层、数据存储层等不同层次数据存储加密需求的数据存储加密架构； 5）建立在线/离线的多级数据归档方式，支持海量数据的有效归档、恢复和使用；

	6）为不同时效性的数据建立分层的数据存储方法，具备按时效性自动迁移数据分层存储的能力； 7）具备数据副本或数据备份存储的多种压缩策略和实现技术，确保压缩数据副本或数据备份的完整性和可用性； 8）存储系统应具备数据存储跨地域的容灾能力； 9）通过工具对需要符合数据存储合规要求的数据进行标识； 10）具备数据时效性自动检测能力，包括但不限于告警、自动删除和拒绝访问等，以保证数据的及时删除、更新和有效性。
5级	1）持续更新优化组织的存储媒体管理系统和净化工具，以保证存储媒体的安全使用； 2）参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆。

（4）数据处理安全技术能力

数据处理安全技术能力包括了数据脱敏、数据分析安全、数据正当使用、数据处理环境安全、数据导入导出安全等方面的能力。以下是对数据处理安全技术能力不同级别的特征描述：

级别	特征描述
1级	无
2级	1）通过一定的技术工具(如敏感字段屏蔽等方式)，实现对核心业务的数据脱敏； 2）核心业务的数据处理环境，应实现了身份鉴别、访问控制、安全配置等； 3）记录组织内部的数据导入导出行为，确保数据导入导出行为追溯。

3级	1）提供统一的数据脱敏工具，实现数据脱敏工具与数据权限管理系统的联动，以及数据使用前的静态脱敏； 2）提供面向不同数据类型的脱敏方案，可基于场景需求自定义脱敏规则； 3）数据脱敏后应保留原始数据格式和特定属性，满足开发与测试需求； 4）对数据脱敏处理过程相应的操作进行记录，以满足数据脱敏处理安全审计要求； 5）在针对个人信息的数据分析中，采用多种技术手段以降低数据分析过程中的隐私泄漏风险，如差分隐私保护、K匿名等； 6）记录并保存数据处理与分析过程中对个人信息、重要数据等敏感数据的操作行为； 7）提供组织统一的数据处理与分析系统，并能够呈现数据处理前后数据间的映射关系； 8）依据合规要求建立相应强度或粒度的访问控制机制，限定用户可访问数据范围； 9）完整记录数据使用过程的操作日志，以备对潜在违约使用者责任的识别和追责； 10）数据处理系统与数据权限管理系统应实现了联动，用户在使用数据系统前已获得了授权； 11）基于数据处理系统的多租户的特性，应对不同的租户保证其在该系统中的数据、系统功能、会话、调度和运营环境等资源实现隔离控制； 12）建立数据处理日志管理工具，记录用户在数据处理系统上的加工操作，提供数据在系统上加工计算的关联关系； 13）记录并定期审计组织内部的数据导入导出行为，确保未超出数据授

	权使用范围； 14）对数据导入导出终端设备、用户或服务组件执行有效的访问控制，实现对其身份的真实性和合法性的保证； 15）在导入导出完成后应对数据导入导出通道缓存的数据进行删除，以保证导入导出过程中涉及的数据不会被恢复。
4级	1）配置脱敏数据识别和脱敏效果验证服务组件或技术手段，确保数据脱敏的有效性和合规性； 2）提供数据脱敏组件或技术手段，支持泛化、抑制、假名化等数据脱敏技术； 3）针对特定的数据使用场景和数据脱敏的策略，部署数据的动态脱敏方案； 4）结合技术手段降低数据分析过程中的安全风险，比如基于机器学习的重要数据自动识别、数据安全分析算法设计等； 5）采取必要的技术手段(如对分析结果数据进行扫描并采取必要的控制措施)和管理措施，避免输出的数据分析结果包含可恢复的个人信息、重要数据等数据和结构标识(如用户鉴别信息的重要标识和数据结构)，以防止数据分析结果危害个人隐私、公司商业价值、社会公共利益和国家安全； 6）建立数据分析过程的安全风险监控系统，对数据分析可能涉及的安全风险进行批量的分析和跟进； 7）具备基于机器学习的敏感数据自动识别、数据分析算法安全设计等数据分析安全能力； 8）在个人信息、重要数据等数据有恢复需求时，采取必要的技术手段

	恢复数据； 9）具备技术手段或机制，对数据滥用行为进行有效的识别、监控和预警； 10）对分布式处理过程中不同数据副本节点数据的完整性和一致性进行定期检测； 11）建立分布式处理节点和用户安全属性的周期性确认机制； 12）建立数据分布式处理节点的服务组件自动维护和管控措施，包括虚假节点监测、故障用户节点确认和自动修复的技术机制； 13）建立分布式处理外部服务组件注册与使用审核机制； 15）具备对密文数据进行搜索、排序、计算等透明处理的技术能力； 16）建立分布式处理过程中的数据泄漏控制机制，防止数据处理过程中的调试信息、日志记录等不受控制输出导致受保护个人信息、重要数据等敏感数据的泄漏； 17）采取多因素鉴别技术对数据导入导出操作人员进行身份鉴别； 18）为数据导入导出通道提供冗余备份能力； 19）对数据导入导出接口进行流量过载监控； 20）建立组织统一的数据导入导出管理系统，提示数据导入导出的安全风险并进行在线审核； 21）配置规范的数据导入导出机制或服务组件，明确数据导入导出最低安全防护要求。

5 级	1）持续跟踪业务新需求、数据脱敏新技术和最佳实践、合规新要求新变化等，持续改进数据脱敏规则和手段； 2）实现对非结构化数据、组合数据的数据脱敏； 3）研究并利用新的技术提升对用户的身份及访问管理能力，并通过风险监控与审计实现对数据使用的安全风险进行自动化分析和处理； 4）参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆。

（5）数据交换安全技术能力

数据交换安全技术能力包括了数据共享安全、数据公开安全、数据接口安全等方面的能力。以下是对数据交换安全技术能力不同级别的特征描述：

级别	特征描述
1 级	无
2 级	采用技术工具实现对数据接口调用的身份鉴别和访问控制。

3级	1）采取措施确保个人信息在委托处理、共享、转让等对外提供场景的安全合规，如数据脱敏、数据加密、安全通道、共享交换区域等； 2）对共享数据及数据共享过程进行监控审计，共享的数据应属于共享业务需求且没有超出数据共享使用授权范围； 3）明确共享数据格式规范，如提供机器可读的格式规范； 4）建立数据发布系统，实现公开数据登记、用户注册等发布数据和发布组件的验证机制； 5）具备对接口不安全输入参数进行限制或过滤能力，为接口提供异常处理能力； 6）具备数据接口访问的审计能力，并能为数据安全审计提供可配置的数据服务接口； 7）对跨安全域间的数据接口调用采用安全通道、加密传输、时间戳等安全措施。
4级	1）建立组织统一的数据共享交换系统，提示数据共享交换的安全风险并进行在线审核； 2）配置数据共享机制或服务组件，明确数据共享最低安全防护要求； 3）应建立统一的数据发布系统，提示数据发布安全风险并进行在线审核； 4）建立数据接口安全监控措施，以对接口调用进行必要的自动监控和处理。
5级	1）对发布的数据，建立持续的追踪能力，优化数据发布规程； 2）在对数据接口调用进行必要的自动化监控和处理基础上，及时跟进最近技术及相关制度，进行安全管理和工程过程的持续改进工作； 3）参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为

	行业标杆。

（6）数据销毁安全技术能力

数据销毁安全技术能力包括了数据销毁处置、存储媒体销毁处置、数据接口安全等方面的能力。以下是对数据销毁安全技术能力不同级别的特征描述：

级别	特征描述
1 级	无
2 级	1）采用技术工具对核心业务存储媒体的数据内容进行擦除销毁； 2）核心业务的存储媒体，应仅采用物理销毁的形式进行销毁。
3 级	1）针对网络存储数据，建立硬销毁和软销毁的数据销毁方法和技术，如基于安全策略、基于分布式杂凑算法等网络数据分布式存储的销毁策略与机制； 2）配置必要的数据销毁技术手段与管控措施，确保以不可逆方式销毁敏感数据及其副本内容； 3）提供统一的存储媒体销毁工具，包括但不限于物理销毁、消磁设备等工具，能够实现对各类媒体的有效销毁； 4）针对闪存盘、硬盘、磁带、光盘等存储媒体数据，建立硬销毁和软销毁的数据销毁方法和技术。
4 级	1）数据资产管理系统应能够对数据的销毁需求进行明确的标识，并可通过该系统提醒数据管理者及时发起对数据的销毁； 2）通过技术手段避免对数据的误销毁； 3）由经过认证的机构或设备对存储媒体进行物理销毁，或联系经认证的销毁服务商进行存储媒体销毁工作。

5级	1）持续更新组织的存储媒体销毁工具，以保证存储媒体销毁的效果； 2）参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆。

（二）制定数据安全建设规划方案

在完成对现有数据安全技术状况的全面评估后，应制定一份科学合理、切实可行的数据安全建设规划方案，方案需充分考虑数据处理全生命周期，并区分数据安全技术建设阶段，为企业的数据安全工作指明方向，合理分配资源，确保数据安全目标的实现。以下是制定数据安全建设规划方案的具体工作步骤：

1. 明确规划目标与原则

（1）确定规划目标

依据评估结果和企业的实际需求，明确数据安全建设的具体目标。例如，短期内可以围绕核心业务重点解决重大合规风险问题，满足法律法规基本要求；中期可以依据数据合规管理义务清单，全面满足法律法规要求；长期可以考虑实现数据安全技术的持续优化，引入人工智能、区块链等前沿技术，构建智能化、自适应的数据安全防护体系。规划目标要与企业的战略发展相契合，支持企业业务的稳定运行和持续发展。

（2）确立规划原则：

合规性原则：严格遵循数据合规相关的法律法规、行业标准和监管要求，确保数据安全建设符合法律规定，避免因违规行为带来的法律风险。

整体性原则：从企业数据安全的整体出发，考虑数据生命周期的各个环节以及与数据相关的人员、技术、管理等要素，制定全面、系统的规划方案，避免出

现安全管理的漏洞和短板。

风险导向原则：以评估出的风险为导向，优先解决高风险问题，合理分配资源，对不同风险等级的数据和系统采取相应的安全措施，提高数据安全建设的针对性和有效性。

成本效益原则：在规划数据安全建设时，充分考虑投入成本与预期效益之间的平衡。选择合适的安全技术和产品，避免过度投资，确保每一项安全措施都能带来相应的价值回报。

持续改进原则：数据安全环境不断变化，规划方案应具有一定的灵活性和可扩展性，能够随着技术的发展、业务的变化以及新的安全威胁的出现而及时进行调整和完善。

2. 设计建设规划方案

建设规划方案的设计需要围绕规划目标与原则，结合企业当前技术现状、业务发展战略、资源配置情况、长短期合规建设需求等基本情况确定。以下规划方案思路仅供参考：

（1）建设阶段划分

基础建设阶段（1年–2年）：重点解决重大合规风险问题，建立基础的数据安全技术体系。具体可以包括完成数据分类分级和基本的访问控制设置，建立初步的安全审计机制；面向用户的前端设备和应用程序数据采集和传输合规，个人信息主体的权利响应机制保障；部署敏感数据加密、脱密等数据防泄漏技术措施；对应用间数据交互进行全面监测，及时发现接口漏洞与异常操作行为；对生产数据导出文件/监管报送文件的产生、存储、使用，外发进行分级标记、全过程管控与追踪溯源；对人员对数据库的操作进行控制和监测，及时发现高危及异

常操作行为；做好基础的数据备份和恢复能力建设等。

优化提升阶段（2–3 年）：进一步优化数据安全技术体系，依据数据合规管理义务清单，全面满足法律法规要求。具体可以包括提升访问控制的精细化程度和数据管控和审计技术的应用水平；建立数据库侧的防护措施，防止后台特权用户违规数据操作；在数据存储阶段，升级加密技术和密钥管理系统，重要的数据建立多个副本；在数据处理阶段，扩大数据脱敏和匿名化的应用范围，进一步控制数据非法使用的风险；在数据交换阶段，建立严格的数据交换授权管理和安全防护机制，做好第三方数据接口的安全监测和全生命周期管理；在数据销毁阶段，配置必要的数据销毁技术手段与管控措施，确保以不可逆方式销毁敏感数据及其副本内容。

创新发展阶段（3 年以上）：引入人工智能、区块链等前沿技术，构建智能化、自适应的数据安全防护体系。全面提升精细化、便捷化安全防护水平，建设集中管控能力，形成全面覆盖数据生命周期的事前防护、事中监测与管控、事后审计溯源能力，支撑持续化运营。实现智能的风险评估和预警，利用区块链技术实现数据的可信溯源和共享。同时，持续关注数据安全技术的发展趋势，不断优化和完善数据安全建设方案。

（2）方案设计要点

数据安全技术体系以覆盖全生命周期安全技术为核心，以支撑全生命周期各环节的通用安全技术为基石，以平台化的协同计算、安全监测与安全运营为总控，形成完备的识别、监测与防护的技术体系。以下是数据处理不同环节设计要点介绍：

①数据收集

数据收集技术措施主要是保障收集过程的数据完整性和数据来源可追溯，不得超范围收集数据。个人信息数据收集时应按照“明确告知、授权同意”的原则

实施，并建立保障个人信息主体知情权、决定权的技术保障机制，若业务停止，则相关收集活动应立即停止。

1）来源鉴别与标记

数据收集源头的安全是数据价值利用的先决条件，在收集外部相关方数据的过程中，应对数据提供方的身份进行有效验证，需明确收集数据的目的和用途，确保数据源的真实性、有效性和最小必要等原则要求，并规范数据收集的渠道、数据的格式以及相关的流程和方式，并标记收集数据的来源，从而保证数据收集的合规性、正当性和执行上的一致性，符合相关法律法规要求。

2）完整性校验

采取完整性校验算法对数据收集进行校验，防止数据在收集过程中被篡改和破坏，保护数据收集的完整性，应对数据收集设备进行持续的身份认证，对数据质量的一致性、完整性、准确性等属性进行监控和管理。

3）最小必要原则

个人信息处理者在收集个人信息前，应在满足 GB/T 35273-2020《信息安全技术个人信息安全规范》中第 5 条关于收集的要求基础上，按照最小必要原则明确收集的个人信息范围，收集的个人信息应限于实现处理目的所必要的最小范围；应采取对个人权益影响最小的方式收集个人信息；应仅在用户使用业务功能期间，收集该业务功能所需的个人信息；如有法律明确规定或经公司内部评估确有必要收集敏感个人信息的，需在通过个人信息保护影响评估之后方可执行；收集个人信息应按照业务核心功能或主要服务，进行分项收集。

4）过度收集监测

针对组织数据和个人信息收集，检验其符合最小必要原则，判断其对组织数据和个人信息的主体合法权益造成损害的各种风险，对收集数量进行监测，过度收集情况及时告警。

②数据传输

应明确数据传输相关安全管控措施，如传输通道加密、数据内容加密、数据接口传输安全、数据传输终端身份鉴别等。对数据传输两端进行身份鉴别，确保传输双方可信任。采用校验技术保证数据在传输过程中的完整性，同时通过网络设备的备份建设确保传输网络可用。

1）传输安全通道

组织内外部在传输数据前，应评估传输通道的安全性，比如从数据传输加密、传输完整性保护、网络可用性等方面进行评估，发现可能存在的数据传输安全风险和违法违规问题，根据数据分类分级传输管理规定和已有数据安全防护措施部署，设计相应的数据传输策略，选择传输安全通道。

2）传输内容加密

根据法律法规、商业合同中的要求和业务的需求，明确组织机构内需要加密传输的数据范围和国家认可的加密算法，综合实现效果和成本，采取相应的数据加密模块，根据不同数据类型和级别进行数据加密处理，并定期审核并调整数据加密算法或密钥。

3）完整性校验

采取完整性校验算法对数据传输的发送和接收进行校验，保护数据传输的完整性，发现数据在传输过程中被篡改和破坏了，要有执行恢复控制的技术能力。

4）传输鉴别

双向传输数据要对传输通道两端进行主体的身份鉴别和认证，部署独立的公钥/私钥对和数字证书，以保证各节点有效的身份认证。

5）传输网络可用性

通过网络基础链路、关键网络设备的备份建设，实现网络的高可用性，从而保证数据传输过程的稳定性。

③数据存储

明确数据存储相关安全管控措施，针对不同类别级别的数据采取差异化安全存储保护措施，如加密、访问控制等。针对存储介质提供有效的技术和管理手段，防止对介质的不当使用而引发数据泄露风险。明确数据备份与恢复安全策略，建立数据备份恢复操作规程，保障数据的可用性和完整性。

1）数据存储加密

存储作为 IT 数据基础设施的底座，对保障数据安全可靠尤为重要。数据库加密技术保障结构化数据存储安全，将明文数据经过加密钥匙（加密密钥）及加密函数转换，变成无意义的密文数据。在加密之后，企业需要获取加密数据内蕴含的信息时，要先将该密文数据经过解密函数、解密钥匙（解密密钥）处理，恢复成原来的明文数据，才能对数据及其内的信息加以使用。

2）存储介质安全

基于组织机构的数据分类分级要求以及介质使用的要求，采取有效的介质净化工具对存储介质进行净化处理，对介质访问和使用行为进行记录和审计。

3）数据备份与恢复管理

明确数据备份与恢复的策略和操作规程，建立用于数据备份、恢复的统一技术，并将具体备份的策略标准化，保证相关工作的自动化执行。建立备份数据的安全管理技术手段，对备份数据的访问控制、压缩或加密管理、完整性和可用性进行管理。

④数据处理

通过用户身份鉴别、数据访问控制、数据展示屏蔽、去标识化、匿名化、数据脱敏等技术手段，保障数据使用和处理安全。在开展数据清洗转换、汇聚融合、分析挖掘等数据加工活动时，应当采用匿名化等措施保护数据主体权益。数据汇聚融合衍生敏感级及以上数据，或导致数据安全级别变化的，应及时评估，并调

整安全保护措施。

1）用户身份鉴别

通过用户身份鉴别识别数据的使用是否得到数据所有者的授权，使用流程是否合规。

2）数据访问控制

数据在使用中发挥价值，但数据在使用过程中的流动性特征，极易导致数据泄露事件的发生。在数据使用阶段，应从数据内容识别和数据细粒度访问控制两方面实施数据安全防护措施，对应用访问数据库的访问控制进行细粒度访问控制。

3）数据展示屏蔽

在数据访问者读取数据的过程中，在应用系统开发的时候，加上数据屏蔽的技术，对敏感数据展示进行遮蔽。

4）去标识化、匿名化

个人信息处理者在对敏感个人信息的展示时，应对需展示的敏感个人信息采取去标识化处理等措施，降低敏感个人信息在展示环节的泄露风险，对于通过匿名化处理的敏感个人信息，应定期评估匿名化处理效果，确保个人信息在当前技术条件下不存在被还原的风险。

5）数据脱敏

数据脱敏分为静态脱敏和动态脱敏，静态脱敏是在生产数据用到测试环节时，要对其中的敏感数据进行脱敏，避免数据泄露。静态脱敏通常会涉及对较大数量的数据进行批量化的处理，静态脱敏系统首先从数据的原始存储环境（通常为生产环境）读入含有敏感信息的数据，然后在非持久化存储条件（系统内存）下按照脱敏策略、规则和算法对数据进行变形等脱敏处理，再将经过处理后的脱敏数据存储到新的目标存储环境中。

6）算法模型安全

采用多种技术手段结合以降低数据加工过程中算法模型安全风险，比如基于机器学习的重要数据自动识别、数据安全分析算法设计、推荐歧视等。

7）加工过程监控

掌握数据安全防护措施部署情况，监控数据加工过程，发现可能存在的数据加工安全风险和违法违规问题。

8）衍生数据分级标记

应对汇聚融合后产生的衍生数据重新开展数据安全定级工作，根据敏感程度打上分级标记，并采用相应级别的安全保护措施。

⑤数据交换

通过隐私计算、机密计算、脱敏等技术保障数据提供和公开安全。建立公开披露数据的审批机制，研判可能产生的影响，数据公开应在官方渠道进行发布，确保数据真实、准确、防篡改，记录审批和发布情况。跨域安全交换同时做好数据溯源标记。

1）隐私计算

数据提供和公开最好做到“数据可用不可见”。隐私计算是“隐私保护计算”的简称，它是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系。从技术机制来看，隐私计算主要分为三大技术路线，即安全多方计算（密码学）、联邦学习。

2）机密计算

机密计算是针对数据在使用过程中的安全问题所提出的一种解决方案，其通过基于硬件的可信执行环境对使用中的数据进行保护，从硬件层面实现对数据以及隐私的保护。其中，可信执行环境被定义为提供一定级别的数据完整性、数据机密性和代码完整性保证的环境。

3）去标识化、匿名化

与数据使用安全部分的相应描述相同，为免赘述，此处略。

4）数据脱敏

敏感数据提供和公开时，采用访问通道上的动态脱敏技术会监测和拦截数据访问请求，并根据请求中数据使用者的角色、权限、待访问数据的类别级别等信息，按照脱敏策略和规则实时对数据展示进行脱敏。

5）跨域安全交换

应保证跨越边界的访问、数据流通过边界设备提供的受控接口进行通信，应在网络边界根据访问控制策略设置访问控制规则，在默认情况下除允许通信外受控接口拒绝所有通信。

6）数据溯源标记

数据一旦提供或公开给其他使用方或处理者，数据所有者可能全面失去数据的管理权和监督权，数据水印技术能够在一定程度上对二次传播的数据进行溯源标记，目前数据水印还不能从根本上阻断数据二次传播。

⑥数据销毁

应按照法律法规、国家标准等有关规定及与数据主体的约定进行数据删除或销毁处理，制定数据销毁管理制度。对存储数据的介质或物理设备采取无法恢复的方式进行数据销毁与删除，明确数据销毁效果评估机制，验证数据删除结果。

1）超限存储匿名化

敏感数据和敏感个人信息存储环境应具备时效性管理能力，应提供过期存储及其备份彻底删除方法和工具，能够验证数据已被删除或被匿名化处理。

2）数据擦除

通过数据覆盖等软件方法进行数据销毁或者数据擦除。数据擦除中的数据软销毁通常采用数据覆写法。数据覆写是将非保密数据写入以前存有敏感数据的硬盘簇的过程。使用预先定义的无意义、无规律的信息反复多次覆盖硬盘上原先存

储的数据，就无法知道原先的数据是“1”还是“0”，也就达到了硬盘数据擦除的目的。

3）物理销毁

涉及敏感数据和个人信息的存储介质销毁时，应采取专业的物理销毁设备进行物理销毁。硬盘数据销毁中的硬销毁则通过采用物理、化学方法直接销毁存储介质，以达到彻底的硬盘数据销毁的目的。

4）删除销毁验证

对于通过匿名化处理的数据，应定期评估匿名化处理效果，确保在当前技术条件下不存在被还原的风险。数据覆写法处理后的硬盘可以循环使用，适应于密级要求不是很高的场合。处理后的硬盘仍有恢复数据的可能，这样就不能达到硬盘数据销毁/数据擦除的效力，因此该方法不适用于存储高密级数据的硬盘，这类硬盘必须实施硬销毁，才能保证彻底的硬盘数据擦除，防止涉密数据的泄露。

（3）资源配置

①人力资源配置

根据不同建设阶段的需求，合理配置人力资源。在基础建设阶段，招聘和培养一批具备基本数据安全知识和技能的人员，负责数据安全技术的实施和管理；在优化提升阶段，引进具有丰富经验的安全专家，对数据安全管理体系进行优化和完善；在创新发展阶段，吸引掌握前沿技术的高端人才，推动数据安全技术的创新和应用。

②资金资源配置

制定资金预算计划，根据建设阶段的不同，合理分配资金。在基础建设阶段，主要资金用于购买安全设备和软件、人员培训等；在优化提升阶段，资金重点投入到技术升级和安全服务购买；在创新发展阶段，资金主要用于前沿技术的研发和应用。

③技术资源配置

选择合适的安全技术和产品，建立技术合作伙伴关系。在基础建设阶段，选择成熟可靠的安全技术和产品，确保数据安全的基本保障；在优化提升阶段，关注技术的更新换代，及时引入先进的安全技术和解决方案；在创新发展阶段，积极探索与科研机构和高校的合作，共同开展前沿技术的研究和应用。

（三）常见数据安全技术工具

数据安全技术工具集按类型总体划分为通用安全类、全生命周期防护类和安全运营与监测平台类三类。其中，通用安全类是对各数据全生命周期处理各个环节技术防护的基础支撑技术，全生命周期防护类是覆盖各数据处理活动环节的安全防护技术，安全运营与监测平台类是对上述各类单点工具的建设与运行进行平台化的统一管控、统一运营、统一监测，形成事前预防、事中监控、事后审计的整体防护效果。

具体的技术工具功能及应用场景简介如下：

1. 全生命周期安全防护类

（1）数据收集安全工具

数据收集的安全工具能够实现对各类终端数据收集设备的接入和数据收集的监控和管理，实现对数据收集设备进行发现和识别、指纹管理、准入与访问控制、网络接入异常监控、数据收集合规分析、流量监控、信令白名单检查等功能。数据收集的安全工具可应用在各数据收集处理活动中。如在互联网数据收集方面，数据安全收集工具能够收集数据收集流量，分析互联网数据收集是否满足合法、合规要求，并对数据收集的终端进行身份认证、数据加密传输、过度收集监测等

进行管控。

（2）数据传输加密技术

数据传输过程保障数据安全采用加密技术，确保数据在传输过程中不被截获、窃取、篡改或伪造。一般传输加密主要使用传输层安全协议（TLS），通过建立安全通道来保护数据的安全性，主要用于远程访问、电子邮件、页面浏览等场景。

国密 TLS：国密 TLS 是应对国内法律法规等相关规定而采用国密的数据安全传输协议，能够兼容传统的 TLS 协议、可实现现有系统的国密改造。国密 TLS1.3 安全强度高且性能优秀，目前已经被国际化标准组织（ISO）和国际电信联盟（ITU）认可，成为国际标准，有很高的国际认可度。

TLS/SSL：SSL（Secure Sockets Layer，安全套接层），用于保障 web 网页通讯的安全。该技术的主要任务是提供私密性、信息完整性和身份认证。TLS（Transport Layer Security，安全传输层协议），用于在两个通信应用程序之间提供保密性和数据完整性。

VPN：虚拟专用网络（Virtual Private Network）的功能是，在公用网络上建立专用网络，进行加密通信。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问，以实现对敏感数据、个人隐私数据在传输过程中的机密性、完整性。

（3）数据防泄漏系统

数据防泄漏（Data Leakage Prevention，DLP）系统又称为数据防泄漏系统，或 DLP 系统。DLP 系统采用内容分析引擎，利用关键字、正则表达式、文件指纹、自然语言处理等数据识别技术，对使用和外发的文件进行解析与扫描，实时识别、监控、保护组织的敏感数据，对即将发生、正在发生的泄露敏感数据行为，按照预置策略及时阻断并告警，监视和保护静止、移动和使用中的数据并防止敏感数据传输到外部，有效避免数据泄露带来的安全风险，最终实现对敏感文件全生命

周期的可知、可见、可控的一体化解决方案。

（4）数据库加密系统

数据库加密系统采用透明加解密、列加密等技术方式，实现对数据库中存储的明文数据进行加密存储、访问权限控制等功能。即使有人想对此类数据文件进行反向解析，所得到的也不过是没有任何可读性的“乱码”，有效避免了因数据库明文存储数据，被拖库而造成数据泄露的问题，从根本上保证数据的安全。数据库加密系统可以应用在数据存储处理活动中。例如，组织的数据高度集中在数据中心，通过对数据库进行加密，能够有效地防止外部非法入侵窃取敏感数据、防止内部高权限用户窃取敏感数据、防止合法用户违规访问敏感数据等由数据明文存储引发的安全风险。

（5）数据备份/恢复工具

数据备份保护是保证数据安全的重要手段，通过备份与恢复有效规避数据丢失或者被窃取的影响。数据备份包括应急容灾、副本管理、数据归档等内容。灾备架构既要能够解决复杂环境带来的脆弱性问题，同时具备多种灾备技术的统一管理，满足动态、敏捷和全面的要求。灾备平台主要用于多种架构下的数据备份和恢复，包括本异地灾备场景、云上数据保护场景、云容灾场景、海量文件备份场景、防勒索病毒场景。

（6）统一身份认证系统

统一身份认证系统（IAM）是一套全面地建立和维护数字身份，并提供有效地、安全地进行 IT 资源访问的业务流程和管理手段，从而实现组织信息资产统一的身份认证、授权、访问控制和身份数据集中管理与审计。统一身份认证系统建设的核心意义在于帮助组织进行应用系统的统一管理，从而提高数据资产的可管理性，也为组织实施进一步的安全保护措施提供支撑。

（7）数据零信任平台

零信任并非没有信任，而是不再简单根据网络位置就判断对资源的访问权限，对何种网络位置均从零开始依靠鉴别与验证建立信任，从而实现纵深防护。保护数据是零信任策略的核心目标，其要求所有用户，无论位于网络内部还是外部，都需要经过身份验证、授权和持续验证，才能访问应用程序和数据，即以动态方式围绕每个连接进行防御，根据风险状态调整访问权限和其他特权。整个数据零信任平台一般由零信任客户端、零信任控制中心和零信任分析中心构成。

（8）数据库运维安全系统

数据库运维安全系统能够将数据库人员身份鉴别、安全策略、访问控制、审批流程管理等有效结合，解决运维账号共享与运维环境共享带来的运维身份不清问题，并且通过精准的 SQL 语句解析技术，建立细粒度的访问操作管控机制，实现对于违反安全策略的风险操作进行拦截、阻断。数据库运维安全系统可以应用在数据使用处理活动中。例如，组织中存在大量的第三方运维、开发商驻场等人员，这些人员一般情况下具有高权限账户，一旦发生高危操作或越权访问，极易造成数据永久丢失、业务中断以及数据泄露等风险，通过部署数据库运维安全系统，可以实现拦截高危操作、防止账户越权访问数据等功能。另一方面，组织的数据库运维关系复杂，存在同一运维人员管理多个账户、多人共享账户等情况，无法针对人员进行最小全向控制并且一旦发生数据安全事件，无法有效定位责任人员，数据库运维安全系统能够通过多维身份认证和登录规则验证的双因素机制有效鉴别运维人员身份，实现授权到人、审计到人、责任到人的溯源机制。

（9）数据库防火墙系统

数据库防火墙系统是基于数据库协议分析与控制技术的增强级数据库安全防护系统，能够主动、实时、全方位地保障数据库安全，使数据免受数据库漏洞、高危恶意操作及敏感数据泄露的威胁。面对来自外部的入侵行为，提供防 SQL 注入和数据库虚拟补丁技术。通过虚拟补丁，使数据库系统不依赖升级、打补丁，

即可完成对主要漏洞的防护。

数据库防火墙系统可以应用在数据使用处理活动中。例如，大小写编码绕过、断包绕过、缓冲区溢出、协议不兼容、参数污染绕过、等价替换绕过等 SQL 注入攻击方式能够穿透传统网络边界防护产品、Web 应用程序输入校验、应用服务器的三层防护，造成刷库、拖库、撞库等数据库安全风险，通过部署数据库防火墙系统，能够基于精准的数据库协议解析技术和控制策略，有效防止 SQL 注入、XSS 攻击等攻击方式；另一方面，在面临端口扫描工具、协议扫描工具、漏洞扫描工具等黑客攻击前的暴露面探测时，能够通过数据库防火墙系统的防端口扫描、防协议扫描等功能，拦截具有端口扫描特征的 TCP/UDP 包、并对协议探测包的特征进行匹配，拦截具有协议探测包。

（10）数据脱敏系统

数据脱敏系统是面向敏感数据进行数据自动发现，按需对敏感数据采取泛化、随机化、抑制、扰乱、加密等一系列技术对源数据进行处理以屏蔽敏感数据，并最大程度保证脱敏后数据的一致性和业务的关联性，满足数据分析、测试开发、数据共享等场景下的数据安全要求。数据脱敏系统根据数据脱敏的实时性和应用场景的不同，分为动态脱敏和静态脱敏。

数据脱敏系统可以应用在数据使用、数据共享、数据公开等多个数据处理活动中。例如，组织在开发测试时，需要使用业务环境中的真实数据进行测试，可以通过数据脱敏系统（静态）采用替换、变形等技术，对源数据中的敏感部分采用相同含义的数据进行替换，如身份证号码脱敏后仍然为有效长度的非真实的身份证号码；在组织进行数据分析时，需要保留数据之间的关联性和分析结果的准确性，可以通过数据脱敏系统（静态）采用抑制、泛化等技术，在脱敏后仍保留原有的数据关系与格式，确保数据脱敏后不会影响分析结果，如多个表格内相同人员的基本信息，脱敏后保持结果一致；另一方面，组织的运维人员、应用侧用

户访问敏感数据时，可以通过数据脱敏系统（动态）采用替换、变形等技术，对源数据中的敏感部分采用相同含义的数据进行替换，如手机号脱敏后仍然为正常长度的非真实的手机号码。数据安全技术发展始终处于对抗与反对抗的博弈中，经过脱敏的数据集仍可能受到隐私攻击的风险，攻击者可通过背景知识、网络公开的身份信息以及黑灰产等渠道获得具备关联信息的数据集，可从脱敏数据集中恢复出原始信息，通常这种攻击被统称为“重标识攻击”，近年来，反“重标识攻击”的防护技术也在不断发展，如通过“K-匿名技术”有效防止数据链接攻击，通过“差分隐私技术”，防止集中数据的差分攻击。

（11）数据安全协同平台

目前不管是多方安全计算还是联邦学习技术，都只能解决单一的隐私计算，无法满足数据充分安全流通、释放数据资产价值的普遍需求。数据安全协同平台是将数据安全协同理念与各种隐私计算技术手段相融合，基于数据分类分级构建具备安全、合规及生态能力的数据共享、研究、利用与交易的平台。该类平台由数据集市、数据安全发布体系、运算资源整合管理与任务调度体系构成，由发布者（数据持有方）在数据集市中通过发布者系统节点发布数据主题服务、参与数据协同任务，由订阅者（数据需求方）在数据集市中通过订阅者系统节点实现数据订阅与发起数据协同任务申请，由协同计算节点根据协同任务需求运用多方安全计算、联邦学习、隐私求交、匿踪查询、数据脱敏等技术实现数据安全共享与交易计算，并通过运算资源整合管理与任务调度体系实现对集市中各方成员的统一管理、计算资源的集中分配、数据共享的集中管控，从而达到“数据不出域、可算不可见”的安全共享与交易。

（12）机密计算平台

机密计算是指在可信硬件支持下的隔离环境中运行安全计算任务，从而对安全计算任务的代码和数据进行保护。机密计算的保护可以让代码和数据免于特权

软件（如操作系统、云虚拟机监控器 Hypervisor）的监视和修改。机密计算通过使用基于硬件的内存保护来改进敏感数据的隔离，能够使被加密的数据在内存中得到处理，降低数据暴露给系统其他部分的风险，从而降低敏感数据泄露的可能性，同时还能为用户提供更高程度的控制和透明使用。

（13）数据水印工具

数据水印工具通过对源数据中嵌入伪行、伪列等水印标记的技术方式，从而在数据进行分发后，能够实现对外发数据进行泄露溯源的功能。数据水印工具能够对外发数据行为进行流程化管理，具备事前数据发现梳理、申请审批、事中添加数据标记、自动生成水印、事后文件加密、外发行为审计、数据源追溯等功能，避免了因内部人员外发数据导致的数据泄露而无法对事件进行追溯的风险，提高了数据传递的安全性和可追溯能力。

数据水印工具应用在数据共享、公开处理活动中。例如，组织内部需要将数据共享至其他部门或第三方，可以通过数据水印工具在源数据中添加伪行、伪列的数据水印，一旦发现数据流传至互联网或其他环境中，可以根据水印信息快速溯源数据泄露源头，能够有效防止数据泄露的风险，提高数据共享的安全性和可追溯能力。在需要进行数据实时交换的应用场景中，可以通过 API 接口的方式调用数据水印工具向特定平台或系统提供数据时嵌入水印，以保证数据的可追溯性。

（14）数据销毁工具

数据销毁工具是指采用各种技术手段将计算机存储设备中的数据予以彻底删除，避免非授权用户利用残留数据恢复原始数据信息，以达到保护关键数据的目的。数据销毁是数据处理全过程的最后一步，主要目的是将计算机或设备在弃置、转售或捐赠前彻底清除所存储的数据，并且无法复原，以免造成信息泄露，保障数据机密性。数据销毁主要分为数据介质物理销毁和逻辑销毁两种。这种技术主要应用于重要或敏感以上数据的销毁处理。一般涉及商业秘密和大量个人信

息的数据在使用完毕后，也应当进行销毁处理。

2. 通用安全防护类

（1）数据资产梳理及分类分级工具

数据资产梳理及分类分级工具通过协议解析、流量分析、敏感数据识别等技术，能够对目标环境中的数据资产进行全面清查、摸排，了解数据资产类型、数据资产分布、数据资产权限、数据资产使用等信息，形成数据资产清单、敏感数据清单。数据资产梳理及分类分级工具通过数据图谱、字段名分析/字段描述分析、表和字段自动关联统计、主从表智能关联、智能化行业数据分类分级知识库等核心能力，能够准确识别数据库中的表/字段的业务含义并与行业数据分类分级标准模板智能建立绑定关系，帮助组织实现智能、快速、便捷的数据分类分级工作。

数据资产梳理及分类分级工具是实现数据安全分类分级保护的核心基础能力。组织需要对数据进行分类分级管理，明确数据的类别和级别，能够进一步明确数据保护对象，有助于分配数据保护资源和成本，是建立完善的数据生命周期保护框架的基础，也是有的放矢地实施数据安全管理的前提条件。

（2）密码基础设施平台

密码基础设施平台通过数字证书作为载体，通过设施、技术、人员、策略、制度、审计的共同作用，实现对网络空间中各类实体的身份和密码机制进行管理，从而为数据安全提供身份的信任机制和数据的加密保护机制，为数据的加密保护提供支撑。

密码基础设施平台具备通用性，能够广泛地为各类业务系统提供数据安全防护。公钥基础设施（PKI）的基于第三方权威的第三方认证，能够保证各类业务

活动中交互双方的身份真实性，PKI 的数字证书和电子签名，能够保证数据的完整性，保证数据不被篡改；PKI 的密钥管理，能够保证数据传递和流通过程不被恶意窃取。

（3）数据库审计系统

数据库审计系统能对旁路镜像流量、虚拟化引流、远程登录、本地流量等多种访问操作数据库方式进行全面审计监测，通过数据库协议解析和深度 SQL 解析技术，实时感知数据库风险，并通过数据库行为建模，基于建模语句的波动情况，可以对数据库访问操作行为进行有效分析和深入挖掘。

数据库审计系统具备通用性，可以帮助组织满足政策合规需求，完善数据安全体系，实现运维侧和应用侧对数据库访问操作全面监测审计，实时告警风险行为，并能够从行为、风险、语句、会话等多维度关联分析挖掘，对数据安全事件精准溯源及定责。

（4）API 监测系统

应用程序编程接口（API）监测系统通过网络流量通讯协议分析和解析、流式计算引擎及高速匹配引擎等核心技术，能够实现应用接口自动发现、涉敏接口自动发现、敏感数据自动发现、接口弱点自动发现等功能，并能够实时监测敏感数据行为、追踪溯源风险事件，帮助组织快速梳理业务应用及接口资产，全面掌握敏感数据访问全貌，及时防控敏感数据行为风险，并通过与数据库审计等系统的配合，能够针对数据泄露事件进行有效溯源。

随着云计算、移动互联网的蓬勃发展，越来越多的应用开发深度依赖于 API 之间的相互调用，API 接口数量飞速增加。API 监测系统能够识别和梳理环境复杂的不同时期、不同业务的众多 Web 应用及 API 接口，帮助组织了解自身应用资产情况；并能够针对互联网用户的应用访问、内部用户的应用访问以及针对敏感数据共享与跨境等场景，发现 API 接口脆弱性，感知 API 接口风险，识别敏感数

据访问流向，减少因 API 接口脆弱性等问题引起的数据泄露。

3. 安全运营平台类

（1）数据安全监测平台

数据安全监测平台是基于数据分析、用户行为分析、可视化分析等技术，从流量、日志等多个维度收集抽取数据，进行关联、分析，构建纵向贯通、横向融通的数据安全监测体系，及时发现、纳管数据库资产和应用资产，识别数据库和业务系统的脆弱性，绘制用户－终端－应用－接口－数据访问的全链路数据流转视图，进一步，基于敏感数据的流转情况，分析攻击特征，建立攻击者身份画像，研判分析安全风险并进行违规告警，同时对风险事件进行数据安全影响分析和追踪溯源，形成数据安全风险趋势预测。

数据安全监测平台的应用场景主要分为三种典型场景，第一种是监管机构对所管辖的单位进行数据安全监管，第二种是集团公司对下属各不同分公司、子公司开展数据安全监管，第三种是组织对本单位的数据安全整体态势进行监测，通过数据安全监测平台，低侵入性持续监测敏感数据流转情况，实时发现数据安全风险，并及时对安全事件进行预警与追踪溯源。

（2）数据安全运营平台

目前数据安全防护手段大多通过提供单一化的功能解决某个方面的问题和需求，这让不同数据安全产品之间的“数据孤岛”现象凸显，继而影响到数据安全建设在落地执行过程中的效率、质量乃至成本投入等诸多层面。

数据安全运营平台作为安全大脑，将管理体系、技术体系和运营体系有机融合，并把分散的数据安全产品能力进行整合，构成“平台化、体系化、可视化、实用化”的一套整体解决方案，帮助组织构建覆盖全生命周期、全领域的数据安

全防控能力，形成对数据资产全链条防护，最终实现常态化、高效的数据安全资产运营、数据安全策略运营、数据安全风险运营、数据安全事件运营机制，不断提升安全运营团队能力。同时通过智能化手段，辅助安全运营人员，提升安全事件的分析和处置能力，从而不断丰富和提升数据安全建设的完整性与成熟度，帮助组织满足监管要求，杜绝敏感数据泄露等安全隐患。

数据安全运营平台通过对各数据安全设备/系统产生及上报的流量日志、事件日志及安全事件等各类日志进行集中化大数据收集、汇聚、存储与归一化解析处理，形成标准化的统一数据格式，以作为支撑数据资产运营、数据安全策略运营、数据安全事件运营、数据安全风险运营的应用、分析与可视化呈现的数据基础。通过用户实体分析技术实现将安全大脑的安全策略发布到各数据安全设备上，并关联端点、网络和应用的自动学习，构建组织的动态数据安全基线，实时监测数据在全生命周期的各处理活动中的安全风险；通过响应与处置自动化技术，联动各数据安全防护产品能力，实现数据安全事件响应和处置，可以协同化、流程化地对一系列安全事件进行告警响应和处置，通过数据溯源技术对数据安全风险进行详尽的追踪溯源。

（3）数据安全评估系统

面对数据安全多法并轨、技术标准并行的情况，目前组织在按合规要求开展数据安全评估工作时，面临评估工作内容繁多、交付周期长、评估服务从业人员门槛较高、评估项目经验难以沉淀的实际痛点，数据安全评估系统基于风险评估开展特性，梳理标准评估实施作业流程，实现评估过程一体化线上统一管理。通过充分自定义的评估调研模板、全面覆盖的评估知识库，结合自动化的检测工具，智能辅助输出评估报告，以实现易管控、更快捷、可沉淀的标准化评估服务工具，降低数据安全评估服务资源投入，提高数据安全评估的效率与准确性。

数据安全评估系统能够面向数据出境、个人信息保护、数据安全能力成熟度

以及安全技术措施专项等多样化场景，以及围绕金融、政务、医疗、企业等不同行业的合规性要求，基于底层的评估知识支撑体系，有效支撑统一化、标准化的自评估及第三方数据安全评估工作的落地，以更好地发挥评估人员的能效，准确高效地评估组织的数据安全管理差距并给出可行的整改建议。

数据安全评估涉及的自动化检测手段目前还仅限于数据库漏扫、API 接口扫描、数据调用链扫描等有限范畴，围绕数据处理活动全面的管理制度、技术措施及安全运营整体评估，仍需持续研究创新自然语言处理、密码算法检测、异常行为识别等人工智能技术在安全评估中的应用，以提高自动化评估检测水平。

通过数据安全建设规划方案的制定和技术措施的部署实施，企业可以多方面提升数据安全防护能力，保障数据在全生命周期内的安全，为数据合规管理体系运行提供有效的技术支撑。同时，随着技术的不断发展和安全威胁的变化，企业应持续关注数据安全领域的动态，及时调整和完善规划方案，确保数据安全工作的有效性和适应性。

第四章 关注数据合规重点工作

本章节将聚焦于数据合规管理中的一些重点工作。网络安全等级保护为企业数据合规运营筑牢安全防线，抵御外部网络攻击与威胁；重要数据识别与管理则帮助企业有效管理重要数据和核心数据，守护国家安全与自身核心利益。个人信息保护影响评估和合规审计，致力于保障个人信息安全，维护用户信任。数据出境合规管理确保企业在全球化进程中，数据跨境流动合法有序。生成式人工智能应用合规管理使企业在享受技术红利时，遵循道德与法律边界。这些重点工作相互关联、相辅相成，共同构建起企业数据合规管理的完整体系，是企业实现可持续发展的必要保障。

（一）网络安全等级保护

网络安全等级保护制度作为国家网络安全保障的基本制度，为企业提供了一套科学、系统的安全管理框架。以分级防护策略为指引，帮助企业合理分配安全资源，确保信息系统和数据承载平台得到有效保护。落实等保制度，不仅能大幅降低企业数据泄露、被攻击的概率，还能凭借规范的安全管理体系，增强客户、合作伙伴对企业数据安全管理的信心，为企业拓展业务、深化合作筑牢坚实的数据安全根基。

1. 法律法规依据

《网络安全法》第二十一条规定国家实行网络安全等级保护制度，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。

《关键信息基础设施安全保护条例》第六条规定运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

《信息安全等级保护管理办法》由公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合制定，详细规定了信息系统安全等级保护的定级、备案、安全建设整改、等级测评、监督检查等工作的流程和要求，是企业开展网络安全等级保护工作的重要指导文件。

《网络安全等级保护条例》（征求意见稿）规定，拟定为第二级以上的网络，

运营者应组织专家评审，有行业主管部门的需报请主管部门核准，跨省或全国统一联网运行的网络由行业主管部门统一拟定等级并组织评审。第二级以上网络运营者在等级确定后 10 个工作日内到县级以上公安机关备案，因网络撤销或变更调整等级的，应在 10 个工作日内办理备案撤销或变更手续。公安机关对备案材料进行审核，对定级准确、材料符合要求的，应在 10 个工作日内出具备案证明。不过，截至目前，《网络安全等级保护条例》尚未正式发布，可能会根据实际情况和各方意见进行进一步的修改和完善。

2. 相关标准

GB/T 22240-2020《信息安全技术网络安全等级保护定级指南》：标准内容围绕定级展开，规定了定级要素，受侵害客体涵盖公民等合法权益、社会秩序公共利益以及国家安全，对客体的侵害程度有一般、严重、特别严重损害之分。依据这些要素，安全保护等级共分五级，从第一级对公民等合法权益造成损害但不危害国家安全到第五级对国家安全造成特别严重危害，逐级递增危害程度。

GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》：标准对不同安全等级的信息系统在安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等技术层面，以及安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等管理层面分别提出了详细的安全要求。这些要求涵盖了身份鉴别、访问控制、安全审计、数据完整性和保密性保护、系统漏洞管理等多个方面，为企业进行信息系统安全建设和整改提供了具体的参照标准。

GB/T 25058-2019《信息安全技术网络安全等级保护实施指南》：该标准为企业实施网络安全等级保护制度提供了详细的操作指南，包括定级、备案、安全建设整改、等级测评、监督检查等各个环节的具体实施步骤和方法。它指导企业

如何根据法律法规要求，结合自身信息系统的特点和业务需求，制定合理的安全策略和方案，确保网络安全等级保护工作的顺利开展。

GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》：明确了对不同安全保护等级信息系统进行等级测评的指标体系和测评方法，规定了测评内容、测评方式、测评流程等方面的要求。测评机构依据该标准对企业的信息系统进行全面评估，判断其是否符合相应等级的安全要求，为企业了解自身信息系统的安全状况、发现安全隐患提供了依据。

GB/T 28449-2018《信息安全技术网络安全等级保护测评过程指南》：详细描述了网络安全等级保护测评的整个过程，包括测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动等。它为测评机构规范开展测评工作提供了指导，确保测评结果的科学性、公正性和准确性，同时也帮助企业更好地配合测评工作，理解测评结果。

3. 关键工作流程

（1）定级

确定信息系统：企业首先需要梳理自身的信息系统，明确纳入等级保护管理的范围。信息系统包括计算机系统、网络设备、数据库、应用程序等相关软硬件设施及其配套的业务应用。

组织定级评审：成立由企业内部相关部门（如信息技术部门、业务部门、安全管理部门等）人员组成的定级小组，按照《信息安全等级保护管理办法》和GB/T22239 等标准的要求，对信息系统的重要性和受破坏后的危害性进行综合分析和评估。考虑因素包括系统所处理数据的敏感性、系统服务的重要性、系统面向的用户群体等。定级小组提出初步的安全保护等级建议，并组织专家进行评审，确保定级结果的合理性和准确性。

审核与批准：将定级结果提交企业决策层进行审核和批准，形成正式的定级报告。对于重要的信息系统，定级结果可能还需要经过上级主管部门或行业监管机构的审核。

安全保护等级初步确定为第一级的等级保护对象，其网络运营者可依据标准自行确定最终安全保护等级，可不进行专家评审、主管部门核准和备案审核。

（2）备案

准备备案材料：对于第二级及以上的信息系统，企业需要准备相关备案材料，主要包括《信息系统安全等级保护备案表》、信息系统拓扑图、系统安全保护策略、管理制度等。备案表中需详细填写信息系统的基本情况、所属单位信息、安全保护等级等内容。

提交备案申请：企业将备案材料提交至当地公安机关网安部门进行备案。公安机关对备案材料进行审核，如发现材料不完整或不符合要求，会通知企业补充或修改。审核通过后，公安机关会发放备案证明，标志着企业的信息系统正式纳入网络安全等级保护管理体系。

（3）建设整改

差距分析：依据 GB/T22239 中对应安全保护等级的基本要求，对信息系统现有的安全保护措施进行全面评估，找出与标准要求之间的差距。分析差距产生的原因，包括技术层面的不足（如缺乏必要的安全设备、安全配置不合理等）和管理层面的问题（如安全管理制度不完善、人员安全意识淡薄等）。

制定整改方案：根据差距分析的结果，制定详细的安全建设整改方案。整改方案应明确整改目标、整改内容、整改措施、责任部门和责任人、整改时间节点等。在技术方面，可能需要增加或升级安全设备（如防火墙、入侵检测系统、数据备份设备等），优化系统安全配置；在管理方面，要完善安全管理制度，加强人员安全培训，建立安全审计机制等。

实施整改：按照整改方案的要求，组织相关部门和人员进行安全建设整改工

作。在整改过程中，要加强对整改工作的监督和管理，确保各项整改措施按时、按质完成。同时，要注意整改工作对业务系统正常运行的影响，采取合理的措施进行风险控制，避免因整改导致业务中断。

（4）等级测评

选择测评机构:企业应选择具备有关资质的等级测评机构对信息系统进行等级测评。测评机构应具有良好的信誉、专业的技术能力和丰富的测评经验。企业可以通过公开招标、竞争性谈判等方式选择合适的测评机构，并签订测评服务合同，明确双方的权利和义务。

配合测评工作：在测评机构进行现场测评时，企业应积极配合，提供必要的支持和协助。包括向测评机构提供相关的技术文档、系统配置信息、安全管理制度等资料，安排技术人员协助测评人员进行测试和检查等。

整改问题：测评机构完成测评工作后，会出具测评报告，指出信息系统存在的安全问题和不符合项。企业应根据测评报告的建议，制定整改计划，及时对存在的问题进行整改，确保信息系统符合相应等级的安全要求。对于短期内无法整改的问题，要制定切实可行的风险应对措施，降低安全风险。

（5）监督检查

接受公安机关检查：公安机关作为网络安全等级保护工作的主管部门，会定期或不定期对企业的信息系统进行监督检查。检查内容包括信息系统的安全保护措施落实情况、安全管理制度执行情况、等级测评工作开展情况等。企业应积极配合公安机关的检查工作，如实提供相关资料和信息。

内部自查：企业自身也应建立健全内部监督检查机制，定期对信息系统的安全状况进行自查。自查可以由企业的安全管理部门或内部审计部门组织实施，检查内容与公安机关的检查内容类似。通过内部自查，及时发现和解决安全问题，不断完善信息系统的安全保护措施和管理制度。

4. 注意事项

（1）准确确定安全保护等级

安全保护等级的确定是网络安全等级保护工作的基础，过高或过低的定级都会带来问题。定级过高会导致企业投入过多的资源进行安全保护，增加成本；定级过低则可能无法有效保护信息系统的安全，面临安全风险。因此，企业在定级时要严格按照标准和规范，充分考虑信息系统的实际情况，确保定级准确合理。对于难以确定等级的信息系统，可以咨询专业机构或专家的意见。

（2）注重整改工作的质量和效果

安全建设整改是提升信息系统安全保护能力的关键步骤。企业在整改过程中，要注重整改工作的质量和效果，确保整改措施能够有效解决存在的安全问题。对于整改过程中涉及的新技术、新设备，要进行充分的测试和验证，确保其兼容性和稳定性。同时，要建立整改工作的验收机制，对整改完成的项目进行验收，确保整改工作达到预期目标。

（3）保持持续关注和改进

网络安全是一个动态的过程，随着技术的发展和安全威胁的变化，信息系统的安全状况也会不断变化。企业要保持持续的安全关注，及时了解最新的安全技术和安全威胁，对信息系统的安全保护措施进行及时调整和改进。定期对信息系统进行安全评估和自查，及时发现和解决潜在的安全问题，确保信息系统的安全稳定运行。同时，要加强与相关部门和机构的沟通和协作，共同应对网络安全挑战。

网络安全等级保护是企业数据合规管理的重要基础工作，企业要充分认识其重要性，严格按照法律法规和标准要求，全面、深入地开展各项工作，不断提升信息系统的安全保护能力，为企业的业务发展提供可靠的安全保障。

（二）重要数据识别与管理

重要数据的识别与管理对于企业的数据合规管理而言，不仅是一项重要任务，更是一道必须严守的法律防线。企业只有精准识别并妥善处理重要数据，才能有效抵御重要数据泄露所带来的潜在风险，切实维护国家和社会的整体利益，同时确保自身业务在合法、合规、稳定的轨道上持续运行。

1. 法律法规依据

《网络安全法》第三十七条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。

《数据安全法》规定，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。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。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；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。

《关键信息基础设施安全保护条例》规定，对于关键信息基础设施的运营者，该条例要求其自行或委托专业机构，每年至少对关键信息基础设施进行一次全面的网络安全检测和风险评估。一旦发现安全问题，必须及时进行整改，并按照保

护工作部门的要求报送详细情况。当关键信息基础设施遭遇重大网络安全事件或发现重大网络安全威胁时，运营者应立即按照相关规定采取有效的应对措施，并迅速向保护工作部门和公安机关报告，以最大程度降低安全事件带来的影响。

《网络数据安全管理条例》第六十二条规定，重要数据是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。第二十八规定网络数据处理者处理 1000 万人以上个人信息的，应当遵守重要数据处理者的规定。第二十九条规定网络数据处理者应当按照国家有关规定识别、申报重要数据。网络数据处理者应当履行网络数据安全保护责任。第三十条规定重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。

《数据出境安全评估办法》规定，将涉及重要数据出境的情况列为数据出境安全评估的重点范畴。当企业的数据处理活动涉及重要数据出境时，数据处理者必须通过所在地省级网信部门向国家网信部门申报安全评估，以确保数据在跨境流动过程中的安全性和合规性，防止重要数据在境外泄露或被滥用。

《促进和规范数据跨境流动规定》明确了重要数据识别申报要求，数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

《汽车数据安全管理若干规定（试行）》规定了汽车数据领域的重要数据范围，包括（1）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；（2）车辆流量、物流等反映经济运行情况的数据；汽车充电网的运行数据；包含人脸信息、车牌信息等的车外视频、图像数据；涉及个人信息主体超过 10 万人的个人信息；国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

《工业和信息化领域数据安全管理办法（试行）》规定了工业和信息化领域重要范围，包括：（1）对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等与国家安全相关的重点领域；（2）对工业和信息化领域发展、生产、运行和经济利益等造成严重影响；（3）造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大；（4）引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响；（5）经工业和信息化部评估确定的其他重要数据。

2. 相关标准

GB/T43697-2024《数据安全技术数据分类分级规则》：这是我国在数据分类分级领域的一项重要国家标准。该标准对重要数据给出了明确的定义："特定领域、特定群体、特定区域或达到一定精度和规模的，一旦泄露可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据"。同时，标准附录 G《重要数据识别指南》中还提出了 17 项具体的识别考虑因素，如"直接影响领土安全和国家统一，或反映国家自然资源基础情况，如未公开的领陆、领水、领空数据"等，为企业准确识别重要数据提供了详细的指导和参考依据。

《信息安全技术重要数据识别指南（征求意见稿）》：该标准于 2022 年 1 月 7 日形成正式征求意见稿，在重要数据识别方面也提供了一定的技术支持和参考思路。它强调了重要数据识别过程中应遵循的原则和方法，对企业在数据合规管理中准确界定重要数据的范围具有一定的指导意义。

行业标准：本行业主管部门已经制定了重要数据具体目录的，企业可以以此识别相关经营数据是否落入目录范围，重要数据目录未对外公开的，企业可通过

电话或当面咨询的方式，向主管部门进行核实确认。

3. 关键工作流程

（1）数据初筛

企业要对自身的数据资产进行全面、深入的梳理，详细记录数据的来源、类型、存储位置、处理方式以及与之相关的业务系统等关键信息。可以借助数据清单模板，结合数据流图等工具，将数据在企业内部的流转过程进行可视化呈现，以便更清晰地了解数据的分布和流动情况。依据《数据安全法》及相关行业重要数据目录，对梳理出的数据进行初步筛选。在筛选过程中，综合考虑数据的敏感程度、数据量的大小以及数据所涉及的业务领域等因素，判断哪些数据可能对国家安全、经济运行、社会稳定或公共健康产生潜在影响，从而形成重要数据的候选清单。这一阶段的筛选工作需要严谨细致，确保重要数据不被遗漏。

（2）识别评估

按照 GB/T43697 标准中规定的关联性、价值性和影响程度等原则进行评估。关联性方面，判断数据是否与国家安全、经济运行等关键领域存在紧密联系；价值性方面，评估数据泄露后可能对企业、社会或国家造成的经济损失、社会影响等；影响程度则通过定性和定量相结合的方式，深入分析数据泄露对不同方面的具体影响，如受影响的人群规模、经济损失的量化程度等。通过综合考量这些因素，准确判断数据是否属于重要数据。

（3）分级保护

在评估过程中，详细记录评估的过程和结果，形成一份全面、详实的重要数据安全评估报告。报告内容应包括数据清单、风险点分析、安全措施建议等重要信息。根据评估结果，对重要数据进行分级，一般可分为重要数据和核心数据。形成重要数据目录，包括数据的名称、类型、来源、存储位置、涉及的主体等信

息，以便后续管理和申报。对于不同级别的数据，企业应制定相应的安全保护措施和管理策略，确保重要数据得到有效的保护和管理。

4. 注意事项

（1）落实安全保护义务

重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全管理机构应当制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案；定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件；受理并处理网络数据安全投诉、举报。网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，由网络数据处理者管理层成员担任，有权直接向有关主管部门报告网络数据安全情况。掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训。审查时，可以申请公安机关、国家安全机关协助。

重要数据的处理者因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障网络数据安全，并向省级以上有关主管部门报告重要数据处置方案、接收方的名称或者姓名和联系方式等；主管部门不明确的，应当向省级以上数据安全工作协调机制报告。

（2）提供、委托处理、共同处理场景下的风险评估

重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估。风险评估应当重点评估提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；网络数据

接收方的诚信、守法等情况；与网络数据接收方订立或者拟订立的相关合同中关于网络数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务；采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险。

（3）定期风险评估

重要数据的处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门应当及时通报同级网信部门、公安机关。风险评估报告应当包括网络数据处理者基本信息、网络数据安全管理机构信息、网络数据安全负责人姓名和联系方式等；处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展网络数据处理活动的情况，不包括网络数据内容本身；网络数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性；发现的网络数据安全风险，发生的网络数据安全事件及处置情况；提供、委托处理、共同处理重要数据的风险评估情况；网络数据出境情况等。处理重要数据的大型网络平台服务提供者报送的风险评估报告，还应当充分说明关键业务和供应链网络数据安全等情况。

（4）关注数据动态变化

企业的数据资产是动态变化的，随着业务的发展和系统的升级，可能会产生新的重要数据或对现有重要数据进行修改。企业要建立数据资产动态管理机制，及时更新重要数据清单，并按照规定进行申报变更。同时，要关注行业法规和标准的变化，及时调整数据管理策略，确保企业的数据管理始终符合最新的法规要求。

（三）个人信息保护影响评估

企业业务如涉及个人信息的处理，其处理活动对个人权益可能产生重大影响。个人信息保护影响评估作为一种系统性的评估方法，旨在识别、分析和减轻个人信息处理活动中潜在的风险，确保企业的个人信息处理活动合法、正当、必要，保护个人信息主体的合法权益。

1. 法律法规依据

《个人信息保护法》第五十五条规定，特定情形时个人信息处理者应当事前开展个人信息保护影响评估工作，包括处理敏感个人信息；利用个人信息进行自动化决策；委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；向境外提供个人信息等情形。第五十六条规定了个人信息保护影响评估的内容，包括个人信息的处理目的、处理方式等是否合法、正当、必要；对个人权益的影响及安全风险；所采取的保护措施是否合法、有效并与风险程度相适应。个人信息保护影响评估报告和处理情况记录应当至少保存三年。

《网络数据安全管理条例》进一步细化和落实了个人信息保护相关要求。例如，规定网络数据处理者处理 1000 万人以上个人信息时，需明确网络数据安全负责人和管理机构，在处理个人信息前应通过制定个人信息处理规则的方式依法向个人告知相关内容，且个人信息处理规则应集中公开展示、易于访问并置于醒目位置等，这些都与个人信息保护影响评估密切相关，为评估工作提供了更具体的操作指导。

《未成年人网络保护条例》明确了未成年人个人信息保护相关的要求。第三十一条规定，网络服务提供者为未成年人提供信息发布、即时通讯等服务的，应当依法要求未成年人或者其监护人提供未成年人真实身份信息。第三十二条规定，个人信息处理者应当严格遵守国家网信部门和有关部门关于网络产品和服务必要个人信息范围的规定，不得强制要求未成年人或者其监护人同意非必要的个人

信息处理行为，不得因为未成年人或者其监护人不同意处理未成年人非必要个人信息或者撤回同意，拒绝未成年人使用其基本功能服务。第三十六条规定，个人信息处理者对其工作人员应当以最小授权为原则，严格设定信息访问权限，控制未成年人个人信息知悉范围。该条例还明确了未成年人员个人信息主体权利响应、个人信息安全事件处置、未成年人私密信息保护等要求。

其他相关法规和政策文件：如一些行业监管部门发布的针对特定行业的个人信息保护规定，可能会对该行业内企业的个人信息保护影响评估提出具体的要求和指导。这些法规和政策文件进一步细化和补充了个人信息保护影响评估的法律依据，使企业在不同行业背景下能够更准确地把握评估的标准和要求。

2. 相关标准

GB/T35273—2020《信息安全技术个人信息安全规范》：对个人信息的收集、存储、使用、共享、转让、公开披露等环节的安全要求进行了规范，为个人信息保护影响评估提供了具体的技术和管理参考依据。

GB/T39335—2020《信息安全技术个人信息安全影响评估指南》：是专门针对个人信息安全影响评估制定的国家标准，详细规定了评估的流程、方法和指标等，为企业开展个人信息保护影响评估提供了直接的操作指南。

GB/T44588-2024《数据安全技术互联网平台及产品服务个人信息处理规则》：规定了互联网平台及产品服务个人信息处理规则的基本要求、编制程序、规则内容和发布形式等要求。

GB/T45404-2025《数据安全技术大型互联网企业内设个人信息保护监督机构要求》：规定了大型互联网企业建立和运行个人信息保护监督机构的要求，包括个人信息保护监督机构的设置、职责、工作规则，以及个人信息保护监督机构的成员等要求。

GB/T45392-2025《数据安全技术基于个人信息的自动化决策安全要求》:规定了个人信息处理者进行自动化决策处理活动时,在数据处理及自动化决策相关典型应用场景下的数据安全和个人信息保护义务、自动化决策的透明度、决策结果公平公正、保障个人合法权益等方面的要求。

GB/T45574-2025《数据安全技术敏感个人信息处理安全要求》:规定了敏感个人信息处理通用安全要求。在信息收集环节,严格遵循最小必要原则,要求处理者确保收集目的明确、合理,仅采集与业务目的直接相关的信息,杜绝过度收集行为。在存储阶段,强调采用加密等可靠技术手段,对敏感个人信息进行安全存储,防止信息在静态存储状态下被非法窃取或篡改。当涉及敏感个人信息的使用、加工、传输、提供、公开以及删除等操作时,也都制定了对应的安全规范。针对敏感个人信息处理特殊安全要求,标准也有专门的规定。当处理特定身份信息,像军人身份信息、国家公职人员特定履职信息等,以及不满十四周岁未成年人的个人信息时,设置了更为严格的安全规则。对于未成年人这一特殊群体,充分考虑其认知和自我保护能力的不足,从收集同意、存储管理到使用限制等各个环节,都给予了更为周全的保护措施。

其他相关标准和技术文件:随着个人信息保护技术的不断发展和实践经验的积累,一些行业协会或技术组织可能会发布与个人信息保护影响评估相关的标准、指南或最佳实践。这些文件可以作为国家标准的补充,为企业在特定行业或领域内开展个人信息保护影响评估提供更具针对性的技术支持和参考。

3. 关键工作流程

(1)评估启动

确定触发条件:企业需要明确哪些个人信息处理活动会触发个人信息保护影响评估。《个人信息保护法》第五十五条规定了特定情形时个人信息处理者应当

事前开展个人信息保护影响评估工作。除了法律法规明确规定的情形外，企业还可以根据自身业务特点和风险状况，设定其他可能需要开展个人信息保护影响评估的情况，如处理大量个人信息、涉及个人信息跨境传输等。

确定评估目标和范围：个人信息保护影响评估可用于合规差距分析，也可以用于合规之上、进一步提升自身安全风险管理能力和安全水平的目的。开展个人信息保护影响评估前，应明晰此次评估的目标。可根据所适用的个人信息保护相关法律、法规、政策及标准，分析特定产品或服务所涉及的全部个人信息处理活动与所适用规则的差距。也可以根据所适用的个人信息保护相关法律、法规、政策及标准，对特定产品或服务所涉及的部分个人信息处理活动与所适用规则的差距进行分析。

组建评估团队：企业自行开展自评估，评估团队应包括熟悉个人信息保护法律法规、业务流程、技术架构以及风险管理等方面的专业人员。团队成员可以来自企业的法务部门、信息技术部门、业务部门以及安全管理部门等。评估团队的负责人应具备较强的组织协调能力和专业知识，能够确保评估工作的顺利开展。也可以委托具有专业能力的第三方进行评估，但第三方机构在评估过程中对知悉的国家秘密、个人信息、商业秘密、保密商务信息等数据应当依法予以保密。

制定评估计划：评估计划应明确评估的目标、范围、方法、时间安排以及人员分工等内容。评估方法可以采用定性与定量相结合的方式，如风险矩阵法、专家评估法等。计划需清楚规定完成个人信息安全影响评估报告所进行的工作、评估任务分工、评估计划表。此外，计划还需考虑到待评估场景中止或撤销的情况。具体操作时考虑人员、技能、经验及能力；执行各项任务所需时间；进行评估每一步骤所需资源，如自动化的评估工具等。

（2）信息收集

收集个人信息处理活动相关信息：评估团队需要全面收集与被评估的个人信息处理活动相关的信息，包括个人信息收集、存储、使用、转让、共享、删除等

环节涉及的个人信息类型、处理目的、具体实现方式等，以及个人信息处理过程涉及的资源（如内部信息系统）和相关方（如个人信息处理者、平台经营者、外部服务供应商、云服务商等第三方）。这些信息可以通过查阅企业的相关文档、记录，与业务人员和技术人员进行访谈，以及对信息系统进行审计等方式获取。

（3）数据映射分析

在针对个人信息处理过程进行全面的调研后，形成清晰的数据清单及数据映射图表。数据映射分析阶段需结合个人信息处理的具体场景。调研过程中尽可能考虑已下线系统、系统数据合并、企业收购、并购及全球化扩张等情况。梳理数据映射分析的结果时，根据个人信息的类型、敏感程度、收集场景、处理方式、涉及相关方等要素，对个人信息处理活动进行分类，并描述每类个人信息处理活动的具体情形，便于后续分类进行影响分析和风险评价。

（4）风险识别与分析

识别潜在风险：根据收集到的信息，评估团队需要识别个人信息处理活动中可能存在的潜在风险。这些风险可以包括个人信息泄露、滥用、未经授权的访问、过度收集、错误处理等。例如，在分析数据共享环节时，要考虑共享对象的安全保护能力、共享数据的范围是否合理等因素，识别可能导致个人信息泄露的风险点。

分析风险产生的原因和可能性：对于识别出的潜在风险，评估团队需要分析其产生的原因和可能性。原因可能包括技术漏洞、管理不善、人员疏忽等。通过对风险原因的分析，可以更准确地评估风险发生的可能性，并为制定相应的风险应对措施提供依据。

评估风险的影响程度：评估团队还需要评估风险对个人信息主体权益的影响程度。影响程度可以从个人的自主决定权、隐私权、名誉权、财产权等方面进行考量。例如，个人信息泄露可能导致个人面临骚扰、诈骗等风险，对个人的隐私权和财产权造成严重影响。根据风险的可能性和影响程度，可以对风险进行量化

或分级，以便后续进行风险评价和处理。

（5）风险评价

确定风险等级：根据风险识别和分析的结果，评估团队需要确定每个风险的等级。可以采用风险矩阵法或其他合适的风险评价方法，将风险的可能性和影响程度相结合，划分出高、中、低不同等级的风险。例如，对于可能性高且影响程度严重的风险，可评定为高风险；对于可能性低且影响程度较小的风险，可评定为低风险。

综合评估整体风险：在确定每个风险等级的基础上，评估团队需要对个人信息处理活动的整体风险进行综合评估。考虑不同风险之间的相互关系和累积效应，判断个人信息处理活动是否对个人信息主体的权益构成重大风险。如果整体风险较高，企业需要采取更严格的风险应对措施。

（6）风险处置

制定风险应对措施：针对识别出的风险，评估团队需要制定相应的风险应对措施。风险应对措施可以包括技术措施、管理措施和组织措施等。例如，对于数据泄露风险，可以采取数据加密、访问控制、定期备份等技术措施；对于管理不善导致的风险，可以完善相关的管理制度、加强人员培训等。风险应对措施应具有针对性、可行性和有效性，能够切实降低风险发生的可能性和影响程度。

实施风险应对措施：企业需要按照制定的风险应对措施，组织相关部门和人员进行实施。在实施过程中，要加强对措施执行情况的监督和检查，确保各项措施得到有效落实。同时，要及时对实施效果进行评估，根据评估结果对风险应对措施进行调整和完善。

监测和跟踪风险：即使采取了风险应对措施，企业仍需要对风险进行持续的监测和跟踪。定期对个人信息处理活动进行复查，评估风险是否得到有效控制，是否出现新的风险。如果发现新的风险或原有风险的情况发生变化，企业需要及时调整风险应对措施，确保个人信息处理活动的安全和合规。

（7）形成评估报告

报告内容：评估报告应包括评估的背景、目的、范围、方法、过程、结果以及风险应对措施等内容。报告应详细描述个人信息处理活动的情况，列出识别出的风险及其等级，说明采取的风险应对措施以及实施效果。评估报告还应包含对个人信息处理活动合规性的结论和建议，为企业的决策提供参考。

报告审核与批准：评估报告完成后，需要经过评估团队内部的审核和企业相关领导的批准。审核过程中要确保报告内容的准确性、完整性和客观性。审核通过后，评估报告应作为企业个人信息保护管理的重要文件进行存档，以备后续查阅和监管部门检查。

4. 注意事项

（1）确保评估的全面性和客观性

在开展个人信息保护影响评估时，评估团队应确保评估的全面性，涵盖个人信息处理活动的各个环节和方面。同时，要保持客观性，不受企业内部利益相关方的影响，以事实和数据为依据进行评估。避免遗漏重要的风险点或对风险进行不当的评估，确保评估结果的真实可靠。

（2）关注法律法规和标准的变化

个人信息保护领域的法律法规和标准不断发展和变化，企业需要密切关注这些变化，及时更新个人信息保护影响评估的依据和要求。定期对评估工作进行回顾和调整，确保评估工作始终符合最新的法律法规和标准要求。避免因法律法规和标准的变化而导致企业的个人信息处理活动出现合规风险。

（3）建立持续改进机制

个人信息保护影响评估不是一次性的工作，而是一个持续的过程。企业应建立持续改进机制，根据评估结果和实际情况，不断优化个人信息处理活动的安全

保护措施和管理流程。定期对评估工作进行总结和反思，分析存在的问题和不足之处，提出改进措施并加以实施，持续提升企业的个人信息保护水平。

（4）注重评估结果的应用

评估结果只有得到有效应用，才能真正发挥个人信息保护影响评估的作用。企业应将评估结果纳入到数据合规管理体系中，作为制定政策、完善制度、改进技术措施的重要依据。同时，要将评估结果与企业的业务决策相结合，确保个人信息保护与业务发展相协调，实现企业的可持续发展。为配合监管活动、增加客户信任，企业可制定个人信息安全影响评估报告发布策略，选择公开发布的个人信息安全影响评估报告可以在已有评估报告基础上予以简化。

个人信息保护影响评估对于保护个人信息主体的合法权益、提升企业的合规水平具有重要意义。企业应严格按照法律法规和标准要求，规范开展个人信息保护影响评估工作，充分认识和重视评估过程中的注意事项，不断完善评估工作机制，确保个人信息处理活动的安全、合规和可持续发展。

（四）个人信息保护合规审计

个人信息保护合规审计是指对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查和评价的监督活动，旨在确保企业的个人信息处理活动符合法律法规的要求，保护个人信息主体的合法权益。通过对个人信息处理的各个环节进行全面审查和评价，可以及时发现并纠正不合规行为，不仅有助于企业降低法律风险，提升社会信任度，还能为企业的可持续发展奠定坚实基础。

1. 法律法规依据

《个人信息保护法》第五十四条规定，个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。第六十四条规定履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。

《网络数据安全管理条例》第二十七条规定，网络数据处理者应当定期自行或者委托专业机构对其处理个人信息遵守法律、行政法规的情况进行合规审计。

《未成年人网络保护条例》第三十七条规定，个人信息处理者应当自行或者委托专业机构每年对其处理未成年人个人信息遵守法律、行政法规的情况进行合规审计，并将审计情况及时报告网信等部门。

《个人信息保护合规审计管理办法》对个人信息保护合规审计活动的开展、合规审计机构的选择、合规审计的频次、个人信息处理者和专业机构在合规审计中的义务等作出细化规定。明确了个人信息处理者自行开展合规审计和按照履行个人信息保护职责的部门要求委托专业机构开展合规审计的条件，以及各自的义务等。

2. 相关标准

目前相关国家标准为全国网络安全标准化技术委员会秘书处 2024 年 7 月 12 日发布的《数据安全技术个人信息保护合规审计要求（征求意见稿）》和 2025 年 4 月 28 日发布的《网络安全标准实践指南—个人信息保护合规审计要求（征求意见稿）》。但该等文件生效版本可能与未生效版本存在较大差异，特别提请

各企业持续关注各文件相关的发布动态。

3. 关键工作流程

（1）审计计划阶段

个人信息处理者可自行开展合规审计，也可委托专业机构进行。处理超过1000万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计。其他个人信息处理者根据自身情况合理确定定期开展个人信息保护合规审计的频次。当履行个人信息保护职责的部门发现个人信息处理活动存在较大风险、可能侵害众多个人的权益或者发生个人信息安全事件时，会要求个人信息处理者委托专业机构开展合规审计。审计主体应根据相关法律法规和企业实际情况，制定详细的审计计划，包括审计目标、范围、方法、时间安排以及人员分工等。明确审计重点关注的个人信息处理环节、涉及的系统和业务流程等。

（2）审计准备阶段

组建审计组：根据组织规模、业务种类、个人信息状况及系统复杂程度组建。内部有专职团队的从团队选派，无则从相关专业能力团队选派，委托第三方时由其组建，内部相关人员可参与支持，任命审计组长统筹工作。

开展审前调查：运用调查表格、查询数据等多种方式，全面了解个人信息处理者的组织架构、处理活动、信息系统、管理制度、安全技术措施以及已发生的安全或违规事件等情况。

确定审计方式方法：采用现场与非现场审计相结合，宜用电子化和自动化审计方式。依据审计对象选择合适方法获取审计证据。

编制和评审审计方案：结合审计对象和方式，识别法规变更更新审计要求，编制审计方案。方案应涵盖被审计单位信息、审计目标范围、流程方法等内容。编制完成后，审计组长和被审计方进行评审，根据评审意见调整，若审计关键要

素变化需重新编制。

（3）审计实施阶段

发送审计通知：正式审计前通知被审计对象负责人，明确审计工作参与者职责、目标范围依据、方法、风险管控、沟通渠道、资源需求、保密安全事项及反馈渠道等。

收集审计证据：审计人员多渠道广泛收集与审计目的相关、如实反映客观情况的证据，并妥善保管、整理成审计底稿。

采信审计证据：仅采信符合要求的审计证据，必要时对取得的材料和对象进行评价分析、技术测试，形成可采信证据并对照形成审计发现。

撰写审计底稿：审计底稿应内容完整、记录清晰、结论明确，反映审计方案实施情况及重要事项，包括审计机构、人员、被审计单位信息，审计事项、程序、发现、结论等内容。

确认审计发现：对审计证据评价分析，定性问题形成审计发现，通过会议通报给管理层并沟通确认。被审计方有异议时协商讨论，必要时核实，若未达成一致则记录在案，同时根据问题影响程度等进行分级排序，审计完成后需被审计方正式确认。

（4）审计报告阶段

异议解决：撰写审计报告前建立异议解决机制，及时沟通确认审计对象提出异议的审计结论，并归档保存沟通结果和结论。

撰写审计报告：审计报告应包含审计概况、依据、过程、结论、发现、意见、建议及其他解释说明材料等内容。审计概况介绍审计项目总体情况；审计依据列出所依据的法律法规等；审计结论对被审计单位合规性等作出评价；审计发现阐述问题事实、定性等；审计意见针对违规情况提出处理意见；审计建议针对问题给出改进措施。

交付审计报告：内部审计报告由审计组长签字提交给组织负责人或个人信息

保护负责人；外部第三方专业机构报告由审计组长、机构负责人签字盖章后，在商定时间内提交。

（5）问题整改阶段

审计人员跟踪审计中发现的不合规项，督促被审计方在规定期限内整改，必要时对整改措施完成情况及有效性进行跟踪审计。

（6）归档管理阶段

个人信息处理者和第三方专业机构妥善保管审计底稿、报告等档案资料。

4. 注意事项

（1）确保审计的独立性和客观性

无论是内部审计人员还是外部专业机构的审计人员，都应独立于被审计的个人信息处理活动，与被审计方无利益冲突。内部审计人员应避免审计自己参与过的项目或工作。如果是委托外部专业机构审计，同一专业机构及其关联机构、同一合规审计负责人不得连续三次以上对同一审计对象开展个人信息保护合规审计，以保证审计结果的公正性和客观性。

（2）保护个人信息和商业秘密

审计人员对在履行个人信息保护合规审计职责中获得的个人信息、商业秘密等依法予以保密，不得泄露或者非法向他人提供。在审计工作结束后，及时删除相关信息，避免信息泄露风险。在审计过程中，严格按照法律法规和企业内部规定的程序进行操作，不得擅自扩大审计范围或获取与审计无关的个人信息。

（3）注重整改效果

个人信息处理者应高度重视审计中发现的问题，将合规审计视为提升自身个人信息保护水平的契机，而不是将其视为一种负担。切实制定并执行有效的整改措施，从制度、流程、技术等方面进行全面改进。通过合规审计，总结经验教训，

建立健全个人信息保护的长效机制。持续加强对个人信息处理活动的监督和管理，定期开展内部培训和宣传教育，提高员工的个人信息保护意识和合规能力，防止类似问题再次出现。

个人信息保护合规审计是企业数据合规管理的重要环节，对于保障个人信息权益、提升企业合规水平具有重要意义。企业应严格按照法律法规和相关标准的要求，认真开展个人信息保护合规审计工作，不断完善个人信息保护措施，促进个人信息的合理利用和安全保护。

（五）数据出境合规管理

数据的跨境流动是助力企业拓展国际业务、参与全球竞争的重要途径。然而，数据出境涉及个人信息保护、国家安全等多方面的重要问题。有效的数据出境合规管理不仅能保障个人信息主体的合法权益，维护国家安全和社会公共利益，还能提升企业的信誉和竞争力。

1. 法律法规依据

《网络安全法》第三十七条规定，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。

《数据安全法》第三十一条规定，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重要数据的出境安全管理，适用《网络安全法》的规定；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。

《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，应当具备下列条件之一：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；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；法律、行政法规或者国家网信部门规定的其他条件。

《数据出境安全评估办法》及申报指南明确了数据处理者向境外提供数据，在涉及重要数据、关键信息基础设施运营者和处理一定规模个人信息的数据处理者等情形下，应当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。

《个人信息出境标准合同办法》及备案指南明确了个人信息处理者可采取签订出境标准合同方式出境的范围以及需要的流程，并明确应当在标准合同生效之日起 10 个工作日内向所在地省级网信部门备案。

《促进和规范数据跨境流动规定》对数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度的施行进行了规定，明确了数据出境合规的客体仅为个人信息或者重要数据，以及免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的多种情形。

《个人信息出境个人信息保护认证办法（征求意见稿）》明确了个人信息出境个人信息保护认证重点评定的内容包括个人信息出境的目的、范围、方式等的合法性、正当性、必要性，境外个人信息处理者、境外接收方所在国家或者地区的个人信息保护政策法律以及网络和数据安全环境对出境个人信息安全的影响等。

《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》规定了个人信息处理者及接收方注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内地部分，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、

中山市、江门市、肇庆市，或者香港特别行政区，在个人信息跨境时可采取签署个人信息跨境流动标准合同方式，并规定了相应的流程。

《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》规定了个人信息处理者及接收方注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内地部分，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，或者澳门特别行政区，在个人信息跨境时可采取签署个人信息跨境流动标准合同方式，并规定了相应的流程。

2. 相关标准

可参考 GB/T 35273—2020《信息安全技术个人信息安全规范》、GB/T 43697—2024《数据安全技术数据分类分级规则》等国家标准来识别个人信息及敏感程度，对数据的重要性和敏感性进行评估，以确定数据出境时的保护级别和合规措施。

3. 关键工作流程

（1）数据出境场景识别与数据梳理

识别场景：数据出境是指数据处理者向境外提供个人信息等数据。一般将数据出境理解为“数据从一法域被转移至另一法域的行为”。根据《数据出境安全评估申报指南（第二版）》，数据出境行为包括：数据处理者将在境内运营中收集和产生的数据传输至境外；数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息等其他数据处理活动。可以通过调研、访谈等形式，全面识别企业已开展或拟开展业务的全部数据出境场景。

梳理数据：列出出境数据清单，包括盘点数据出境所涉及的系统、系统间数

据流转情况、系统所涉及的数据存储情况等；明确出境数据的种类和数据项名称，结构化数据要细化到不可继续拆分的字段，非结构化数据要明确文件名及文件包含或隐含的字段或内容，并提供每个数据项的样例。

（2）数据类型判断与规模统计

判断数据类型：根据行业主管部门、地区关于重要数据的管理要求，参考国家标准、行业标准等，判断出境数据中是否包含重要数据。依据相关标准识别个人信息及敏感程度，如涉及生物识别、宗教信仰等敏感个人信息需特别关注。

统计数据规模：按照行业主管部门有关认定要求，统计拟出境重要数据的数据规模，以及已出境和拟出境个人信息涉及的自然人人数。统计周期为自当年1月1日起累计，数量以自然人为单位去重后的统计结果为准，需分别明确其中包含当年已出境数量和未来新增数量。

（3）合规路径选择

在识别出数据出境的场景后，企业需要根据数据出境的情况选择数据出境的路径，目前分为四类：豁免情形、数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

①数据出境的豁免情形

以下情况无需申报数据出境安全评估、订立个人信息出境标准合同或通过个人信息保护认证：

1）国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的；

2）在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的；

3）为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的；

4）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的；

5）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的；

6）关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息）的；

7）自由贸易试验区内数据处理者向境外提供负面清单外的数据。

②适用数据出境安全评估的情形

企业向境外提供数据，有下列情形之一的，应当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：

1）关键信息基础设施运营者向境外提供个人信息或者重要数据；

2）关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息；

③适用个人信息保护认证及订立个人信息出境标准合同的情形

关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）或者不满1万人敏感个人信息的，应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证。企业不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

（4）境外接收方调研与法律文件拟定

调研境外接收方：与境外接收方沟通，了解其基本情况，包括数据安全保障能力、所取得的相关资质及认证，所在国家或地区的网络和数据安全法律法规情况，以及处理数据的全生命周期过程等。

拟定法律文件：根据相关法规要求与境外接收方拟定法律文件，可参考个人

信息出境标准合同拟定，但至少应包含《数据出境安全评估办法》第九条涉及的六项内容；若适用个人信息出境标准合同备案，需使用《个人信息出境标准合同》模板。

数据安全保障能力梳理：梳理数据处理者在数据全生命周期的数据安全管理能力、数据安全技术能力等情况，若涉及去标识化、匿名化等情况，需详细说明。提供相关制度、技术保障措施截图、数据安全有效性证明等文件，以证明企业具备保障数据出境安全的能力。

（5）开展评估

数据出境风险自评估：依据相关法规和指南要求，对数据出境可能面临的风险进行全面评估，包括数据被窃取、泄露、毁损以及非法利用的风险，境外接收方所在国家或地区的法律政策风险等，并形成自评估报告。

个人信息保护影响评估：针对涉及个人信息出境的情况，按照《个人信息保护法》规定，评估数据出境对个人信息主体权益可能产生的影响，提出相应的风险防控措施。

4. 注意事项

（1）全面识别数据出境行为

严格按照法律法规和相关标准，准确判断企业的业务活动是否属于数据出境行为，避免遗漏或错误判断。对于一些边界模糊的情况，如境外机构间接获取境内数据等，要谨慎分析和界定，确保所有应纳入合规管理的数据出境活动都得到有效管控。

（2）关注法规政策变化

数据出境合规相关的法律法规和政策处于不断完善和调整中，企业要密切关注国家网信部门等发布的最新规定、指南和通知，及时调整自身的数据出境合规

策略和措施，以适应新的要求。例如，《促进和规范数据跨境流动规定》对之前的一些规定进行了调整和明确，企业需按照新规定执行。

（3）确保材料真实性和完整性

在申报数据出境安全评估、备案个人信息出境标准合同或申请个人信息保护认证等过程中，企业提交的材料必须真实、准确、完整。提供虚假材料不仅会导致合规工作无法通过，还可能面临法律责任追究。

（4）保护个人信息主体权益

无论选择何种数据出境合规路径，都要把保护个人信息主体权益放在重要位置。在数据出境前，要按照法律规定履行告知、取得个人单独同意等义务，确保个人信息主体的知情权和选择权。同时，要采取必要的技术和管理措施，保障个人信息在境外的安全存储和合法使用，并明确个人向境外接收方行使权利途径和方式。

（5）建立持续监控和应急响应机制

数据出境后，企业要建立持续监控机制，定期对数据出境活动进行检查和评估，及时发现可能出现的风险和问题。一旦发生数据安全事件，要立即启动应急响应机制，采取有效的补救措施，降低损失和影响，并按照规定向有关部门报告。

（6）遵守出口管制要求

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，企业向境外提供涉及出口管制的数据的，应当依法向有关部门申请出口许可证；可能危害国家安全和利益的，不得向境外提供。

（7）境外司法或执法机构调取数据场景下的合规义务

非经中华人民共和国主管机关批准，企业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。

企业数据出境合规管理是一个复杂且重要的工作领域，随着数据在全球范围内的流动日益频繁，相关的法律法规和监管要求也在不断发展和完善。企业必须高度重视数据出境合规管理，严格遵循适用的国家法律法规和相关标准，密切关注并妥善处理各项注意事项。通过加强内部管理、提升技术能力、增强员工合规意识等多方面的努力，确保数据出境活动的安全、合法、有序，实现企业发展与数据合规的良性互动。只有这样，企业才能在全球数字化竞争中赢得主动，实现可持续发展的目标。

（六）生成式人工智能应用合规管理

生成式人工智能（AIGC）以其强大的创造力和广泛的应用前景，深刻改变着各行业的运作模式和社会的发展格局。从智能创作、虚拟客服到医疗诊断辅助、金融风险预测等领域，生成式人工智能正发挥着日益重要的作用。然而，生成式人工智能技术应用面临虚假信息、数据侵权、算法歧视等法律风险。我国《生成式人工智能服务管理暂行办法》《互联网信息服务深度合成管理规定》《互联网信息服务算法推荐管理规定》《人工智能生成合成内容标识办法》等法规明确要求，AIGC 服务提供者须履行算法备案与安全评估的强制义务，覆盖数据来源合法性、内容审核机制及用户权益保护等核心环节。未合规企业可能面临高额罚款、业务暂停等行政处罚，并需承担民事侵权责任。

1. 合规依据

《生成式人工智能服务管理暂行办法》：明确了生成式人工智能服务的定义、适用范围和监管原则，强调服务提供者需对训练数据的合法性、真实性和安全性负责，采取有效措施防止数据污染和泄露。同时，要求服务提供者建立健全内容

审核机制，确保生成内容符合法律法规和公序良俗。

《互联网信息服务深度合成管理规定》：聚焦于深度合成技术在互联网信息服务中的应用，对深度合成服务提供者的主体责任、技术管理、内容审核、用户管理等方面作出了具体规定。特别强调了对深度合成内容的标识要求，以增强信息的透明度和可追溯性。

《互联网信息服务算法推荐管理规定》：针对算法推荐服务进行全面规范，要求算法推荐服务提供者建立健全算法机制机理审核、科技伦理审查、用户注册、信息发布审核、数据安全和个人信息保护等管理制度和技术措施。明确了算法备案的具体要求和流程，以及对具有舆论属性或社会动员能力的算法推荐服务的安全评估要求。

《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》：当生成式人工智能应用的服务具有舆论属性或社会动员能力时，需依据此规定进行安全评估。评估内容包括服务的安全管理制度、技术保障措施、信息发布审核机制、应急处置预案等方面。通过安全评估，及时发现和解决潜在的安全风险，确保生成式人工智能应用在传播信息、引导舆论等方面的安全性和合规性。

《网络信息内容生态治理规定》：旨在营造良好的网络信息内容生态环境，生成式人工智能生成的内容也属于网络信息内容的范畴。规定明确了网络信息内容生产者、服务平台和使用者的权利、义务和责任，要求生产者不制作、不发布、不传播违法有害信息，服务平台要履行信息内容管理主体责任，建立健全信息内容审核机制，使用者要文明使用网络，不传播违法有害信息。生成式人工智能服务提供者和使用者都应遵守这些规定，共同维护网络信息内容生态的健康有序。

《科技伦理审查办法(试行)》：强调科技活动应遵循伦理原则，生成式人工智能作为一项重要的科技应用，其研发和应用过程需进行科技伦理审查。审查内容包括对人类尊严、社会公平、生态环境等方面的影响评估，确保生成式人工智能的发展符合伦理道德要求，不损害人类的根本利益和社会公共利益。

《人工智能生成合成内容标识办法》：进一步明确了对人工智能生成合成内容的标识要求，与《互联网信息服务深度合成管理规定》相呼应。通过标识，使用户能够清晰识别生成合成内容，增强信息的透明度，减少信息误导和欺诈的可能性。同时，也有助于监管部门对生成合成内容进行有效管理和监督。

2. 相关标准

GB/T41867-2022《信息技术人工智能术语》：作为人工智能领域的基础术语标准，为生成式人工智能应用管理提供了统一的术语定义和解释。在法规执行、标准制定、技术研发和应用推广等过程中，准确理解和使用相关术语是确保各方沟通顺畅、管理有效、技术创新的重要基础。

GB/T42888-2023《信息安全技术机器学习算法安全评估规范》：对机器学习算法的安全评估提供了详细的规范和方法，生成式人工智能所依赖的算法也需遵循该标准进行安全评估。通过对算法的安全性、可靠性、隐私保护等方面进行评估，及时发现算法中存在的安全漏洞和风险，采取相应的措施进行改进和优化，提高算法的安全性和可信度

GB45438-2025《网络安全技术人工智能生成合成内容标识方法》：该标准为人工智能生成合成内容的标识提供了具体的技术方法和规范。详细规定了标识的内容、格式、位置、实现方式等方面的要求，确保标识的准确性、可读性和可追溯性。生成式人工智能服务提供者可依据此标准对生成的内容进行标识，提高内容的可识别性和管理效率。

GB/T45654-2025《网络安全技术生成式人工智能服务安全基本要求》：适用于生成式人工智能服务提供者开展相关服务活动，同时也为相关主管部门以及第三方评估机构提供参考依据。该标准明确了生成式人工智能服务需遵循的网络安全基本要求，涵盖训练数据安全方面，要求服务提供者确保训练数据来源合法、

合规，具备完整性、准确性校验机制，防止数据泄露与被篡改；模型安全层面，要对模型进行安全评估与加固，避免模型被恶意攻击、逆向工程等风险；安全措施领域，制定了访问控制、加密通信、应急响应等一系列保障机制，并针对各项基本要求给出了相应的评估方法，以便精准衡量服务的安全合规程度。

GB/T45674-2025《网络安全技术生成式人工智能数据标注安全规范》：主要针对生成式人工智能数据标注组织方开展训练数据标注活动进行规范，生成式人工智能数据需求方在对数据标注进行检查、验收，以及第三方机构对数据标注进行安全性评估时也可参照执行。标准详细规定了数据标注平台或工具需具备的安全防护能力，如身份认证、访问控制、数据加密存储等；数据标注规则应科学合理，避免引导标注人员产生错误或偏见标注；对数据标注人员在资质审核、安全培训、操作规范等方面提出要求；明确数据标注核验流程与标准，保证标注结果质量。此外，还给出了数据标注安全评价方法，助力各方对标注工作安全性进行量化评估。

GB/T45652-2025《网络安全技术生成式人工智能预训练和优化训练数据安全规范》：适用于生成式人工智能服务提供者开展预训练和优化训练数据处理活动以及安全自评估，第三方机构对预训练和优化训练数据进行安全性评估时也可参考此标准。标准提出了预训练和优化训练数据的通用安全要求，包括数据的合法性、合规性保障，数据质量把控等；对预训练数据处理活动，从数据收集、清洗、标注到存储、传输等环节制定安全要求；针对优化训练数据处理活动，也明确了在模型微调、增量训练等过程中的数据安全规范，并给出对应的评价方法，以此确保生成式人工智能训练数据全生命周期的安全性。

3. 合规建设要点

（1）制度建设与管理

依据相关规定，建立涵盖用户注册、算法审核、科技伦理审查、信息发布审核、数据安全、个人信息保护、应急处置等方面的管理制度。明确各部门和岗位在人工智能服务中的职责和工作流程，确保各项规定得到有效执行。制定并公开管理规则、平台公约和服务协议，以显著方式提示用户承担信息安全义务，明确双方权利义务，包括对生成内容的使用限制、知识产权归属、用户信息保护等内容。

（2）数据管理

依法开展训练数据处理活动，使用具有合法来源的数据和基础模型，确保涉及知识产权的数据不侵权，涉及个人信息的数据取得同意或符合法定情形，采取措施提高训练数据质量。完善数据安全管理措施，采取加密、访问控制、数据备份等技术措施，保障训练数据和用户数据的安全，防止数据泄露、篡改和丢失。对包含个人信息的数据，严格遵守个人信息保护的有关规定。

（3）算法与技术管理

定期审核、评估、验证生成合成类算法机制机理，确保算法符合法律法规和伦理道德要求，不设置诱导用户沉迷、过度消费等违反规定的算法模型。对具有舆论属性或者社会动员能力的算法，按要求履行备案和变更、注销备案手续。

按照相关规定，对生成合成内容添加显式标识和隐式标识。在文本、音频、图片、视频等不同类型的生成内容中，根据各自特点在适当位置添加显著的提示标识，同时在文件元数据中添加隐式标识，包含生成合成内容属性信息、服务提供者名称等制作要素信息。

（4）用户管理与服务

基于移动电话号码、身份证件号码等方式，依法对用户进行真实身份信息认证，不得向未认证用户提供信息发布服务。保护用户的合法权益，包括提供安全、稳定、持续的服务，保障用户正常使用。建立便捷的用户申诉和公众投诉、举报入口，及时受理、处理并反馈处理结果。

（5）安全评估与监督

提供具有舆论属性或者社会动员能力的生成式人工智能服务的，按国家有关规定开展安全评估。在开发上线新产品、新应用、新功能时，同样要进行安全评估。有关主管部门开展监督检查时，企业应依法予以配合，按要求对训练数据来源、算法机制机理等予以说明，并提供必要的技术、数据等支持和协助。

（七）反不正当竞争、反垄断及商业秘密保护

企业在生产经营活动中涉及向第三方提供或从外部获取数据的情形，需高度关注《刑法》《反不正当竞争法》《反垄断法》等法律框架下的合规义务。现行法律虽未穷尽列举数据领域不正当竞争行为的构成要件，但最高人民法院《关于适用〈反不正当竞争法〉若干问题的解释》（法释〔2022〕9号）已确立"商业道德-损害后果-行为关联性"的裁判规则，近几年公布的反垄断、反不正当竞争典型案例更凸显数据滥用行为的法律风险。

近年司法实践中，因擅自抓取第三方数据资源被认定为不正当竞争（如"微博诉脉脉案"）、利用算法实施数据垄断（如"某外卖平台"二选一"案"）、员工泄露企业数据构成侵犯商业秘密罪（如"香兰素技术秘密案"）等案件呈多发态势。请各市场主体以案为鉴，在数据获取、使用、共享等环节建立完善合规体系，避免引发民事赔偿、行政处罚乃至刑事责任。

1.合规依据

《刑法》对侵犯商业秘密罪的构成做出了明确规定，企业存在下列行为的，情节严重或特别严重的，构成侵犯商业秘密罪：（一）通过盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密的；（二）披露、使

用或者允许他人使用以前项手段获取的权利人的商业秘密的；（三）违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的；（4）明知存在前述行为，而获取、披露、使用或者允许他人使用该商业秘密的。《反不正当竞争法》对企业的不正当竞争行为及侵犯商业秘密的行为做出了规定，并对企业不正当竞争行为及侵犯商业秘密行为的民事责任、行政责任做出了规定。其中第十二条规定，利用网络从事生产经营活动，不得利用技术手段，通过影响用户选择或者其他方式，实施妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为。

《反垄断法》对企业的垄断行为及实施垄断行为的民事责任、行政责任做出了规定。国务院反垄断委员会针对《反垄断法》发布的《关于平台经济领域的反垄断指南》第十七条对企业基于大数据和算法，根据交易相对人的支付能力、消费偏好、使用习惯等，实行差异性交易价格或者其他交易条件；实行差异性标准、规则、算法；实行差异性付款条件和交易方式等可能滥用市场支配地位，无正当理由对交易条件相同的交易相对人实施差别待遇，排除、限制市场竞争的行为也进行了规制。

2.合规建设要点

现行司法裁判标准呈现动态发展特征，本合规建议基于最新实践基准形成基础框架。企业应当建立司法动态追踪机制，重点关注反不正当竞争与反垄断领域裁判规则的系统性演进。

（1）关注数据获取途径的合法合规

企业应当优先通过具备法定数据处分权的适格主体获取数据资源。建议优先选择深圳数据交易所等持牌数据交易场所进行合规采购，该类机构已完成数据权属核验、交易备案等法定程序。交易实施前需要求数据供应方提供完整权属证明

文件，包括但不限于《数据来源声明》《数据加工处理证明》及《数据交易授权书》。

（2）协议签署规范

在数据采购协议中应当明确约定数据使用范围、授权期限、再授权限制等核心条款，重点载明数据来源合法性担保条款。

（3）数据爬取行为的合规性

数据爬取行为已构成当前不正当竞争纠纷的重要违法形态，大量不正当竞争纠纷因数据爬取而起。企业在爬取数据时，需重点评估目标网站的robots.txt协议限制层级，对明确禁止爬取的目录或文件应当规避；同时，不得实施影响网络服务正常运行的爬取行为，建议设置合理采集频率，或非法侵入他人信息系统。

此外，企业应系统核查目标网站的《服务协议》《隐私政策》等法律声明，对采取会员认证、付费订阅等访问限制措施的网站，需获得明示授权后方可实施爬取。特别注意不得绕过技术防护措施获取数据，该行为可能构成《反不正当竞争法》第十二条禁止的"妨碍、破坏网络产品与服务正常运行"行为。

（4）数据加工、使用

对获取的原始数据应当实施实质性加工处理，包括但不限于数据清洗（去除无效字段）、结构化处理（建立数据关联模型）、深度分析（构建用户画像）等创造性劳动。在数据加工过程中应当建立原始数据存档机制，确保数据加工处理过程可追溯。禁止实施歪曲数据本意、篡改数据关联关系等可能造成误导性结论的操作。

使用爬取数据开发的产品或服务，需与数据来源方主营业务进行竞争关系评估。若构成直接竞争关系，需确保数据使用行为未违反《反不正当竞争法》第二条规定的商业道德准则。

（5）反垄断

企业开展数据与算法应用时，应当严格遵守《反垄断法》相关规定：如禁

止实施滥用市场支配地位行为，包括但不限于：利用技术或数据优势实施排他性竞争；不当限制交易对象选择权；强制实施排他性交易（如"二选一"协议）。

同时，在使用算法时应注意公平性规范，注意防范算法歧视风险，可关注以下重点：禁止基于用户特征实施差异性定价（"大数据杀熟"）；建立价格算法公平性校验机制；对特殊群体实施保护性算法策略。

出现差异性对待时，应考虑其合法性要件实施差别化对待时应履行合理性评估义务，符合以下情形可认定具有正当性：基于交易相对方实际需求且符合正当交易习惯；针对新用户开展的限时优惠活动；依据公示规则实施的随机性交易；能够证明符合商业伦理的其他正当理由。

第五章 运用数据合规建设成果

本章节将阐述数据合规建设成果对企业的积极影响。企业通过前期在识别数据合规管理义务、建立合规组织、制定管理制度、完善安全技术措施以及规范运营过程等方面的不懈努力，积累了丰富的数据合规建设成果。如何充分运用这些成果，对于维护企业合法权益、提升企业品牌形象、促进数据资产管理、推动新兴技术应用具有深远意义。

（一）维护企业合法权益

充分运用数据合规建设成果来维护企业合法权益，不仅是企业应对外部监管的需要，更是保障自身可持续发展的关键。这些数据合规风险管控措施的有效实施，不仅有助于企业降低数据处理过程中的风险，避免因数据违规行为引发的法律纠纷和经济损失，还能显著降低企业的整体经营风险，为企业营造稳定、健康的发展环境。以下是运用数据合规建设成果维护企业合法权益的具体工作建议：

1. 建设成果与权益关联

企业需全面梳理数据合规建设成果，基于合规建设成果分析哪些成果与企业的数据权益保护直接相关。确定在数据资源持有权、数据加工使用权、数据产品经营权等方面，合规成果是如何发挥作用的。将数据合规建设成果与企业的数据权益进行一一对应，建立关联矩阵。通过这种方式，清晰地展示出各项合规建设成果对不同权益保护的具体贡献，为后续的权益维护工作提供明确的指引。

2. 应对外部权益侵害与纠纷

（1）建立监测机制

利用数据合规建设中建立的监测系统和技术手段，对企业的数据权益进行实时监测。关注数据的访问日志、异常流量、数据泄露预警等指标，及时发现潜在的权益侵害行为。例如，通过入侵检测系统（IDS）和安全信息与事件管理系统（SIEM），实时监测网络流量和系统活动，一旦发现异常情况，立即发出警报。

（2）制定应对策略

针对可能出现的权益侵害行为，制定相应的应对策略。根据侵害行为的性质

和严重程度，确定采取的措施，如警告、协商、法律诉讼等。在制定策略时，充分考虑企业的利益和声誉，以及相关法律法规的规定。例如，对于轻微的侵权行为，可以先发出警告，要求对方停止侵权行为并采取补救措施；对于严重的侵权行为，则果断采取法律诉讼的方式维护企业的权益。

（3）证据收集与保存

在应对权益侵害和纠纷时，企业应利用数据合规管理过程中建立的证据留存机制，及时收集和保存与权益侵害相关的证据，如数据访问记录、通信记录、合同文件等。确保证据的真实性、完整性和合法性，为后续的法律程序提供有力支持。例如，在数据泄露事件中，及时保存系统日志、监控录像等证据，以便查明泄露原因和责任方。

（4）法律支持与合作

充分发挥企业内部法务部门的作用，同时适时聘请外部的法律顾问，为企业在权益维护方面提供专业的法律支持。法律顾问可以帮助企业分析权益侵害行为的法律性质和后果，制定合理的法律策略，代表企业参与诉讼或仲裁等法律程序。

（5）法律责任减免

通过切实履行相应的合规义务，企业不仅能够在面对潜在法律纠纷时更好地维护自身权益，还能在符合相关法定条件的前提下，依据涉案企业合规的相关制度，争取从轻或者减轻行政处罚的机会。同时，当面临民事侵权指控时，完备的合规措施可作为企业已尽合理义务的有力证明，从而有可能使企业免于承担侵权责任。

①合规从轻或者减轻行政处罚

《行政处罚法》第三十二条规定，“当事人有下列情形之一，应当从轻或者减轻行政处罚：（一）主动消除或者减轻违法行为危害后果的；（二）受他人胁迫或者诱骗实施违法行为的；（三）主动供述行政机关尚未掌握的违法行为的；（四）配合行政机关查处违法行为有立功表现的；（五）法律、法规、规章规定

其他应当从轻或者减轻行政处罚的”。《行政处罚法》第三十三条第一款规定，“违法行为轻微并及时改正，没有造成危害后果的，不予行政处罚。初次违法且危害后果轻微并及时改正的，可以不予行政处罚”，该条第二款规定，“当事人有证据足以证明没有主观过错的，不予行政处罚。法律、行政法规另有规定的，从其规定”。据此，《行政处罚法》规定了从轻、减轻、不予行政处罚的措施和情形。

②举证证明尽到合理义务不承担侵权责任

《网络安全法》《个人信息保护法》《数据安全法》等法律法规、部门规章等规范均规定了企业需要履行的法定义务，该等义务涵盖网络安全等级保护测评、个人信息保护影响评估、个人信息保护合规审计、数据分类分级、数据安全风险评估、数据加密存储和传输、访问控制、应急预案及演练、数据安全教育培训、网络/数据安全事件分级管理、安全事件处置和报告、网络日志留存符合法律法规规定等法定义务。而根据前文所述，在发生侵权等民事纠纷时，法院原则上会推定企业存在过错，需要企业举证证明自己没有过错方可免除承担侵权责任，与之相应，如果企业完成了数据合规管理体系建设，落实相关安全和合规义务，并对合规管理过程留下详细记录，在发生民事纠纷时，能够举证证明自己尽到了合理义务，则企业可以免除承担相应的民事法律责任。

3. 参与行业权益保护与标准制定

企业应积极关注行业内的数据权益保护动态和趋势，了解其他企业在权益保护方面的经验和做法。参与行业协会组织的研讨会、论坛等活动，与同行企业进行交流和分享。根据企业自身的数据权益保护需求和实践经验，向行业协会、监管机构等提出合理的权益诉求和建议。参与行业标准和规范的制定过程，将企业在数据合规管理方面的良好实践和经验纳入标准中，推动行业整体的数据权益保

护水平的提升。也可以与其他企业建立合作关系或联盟，共同应对数据权益保护方面的挑战。通过合作，可以共享资源、技术和经验，提高企业在权益保护方面的能力和影响力。

（二）提升企业品牌形象

完成数据合规管理体系建设并完善相关技术措施后，企业拥有了坚实的数据合规基础。充分运用这些成果，不仅能确保企业合法合规运营，更能显著提升企业的品牌形象，赢得市场和客户的青睐。

1. 通过权威认证，提升品牌公信力

（1）ISO27001 信息安全管理体系认证

ISO27001 是国际上被广泛认可的信息安全管理标准。企业通过该认证，表明其在信息安全管理方面达到了国际先进水平。在实践中，企业需依据 ISO27001 的要求，建立完善的信息安全管理体系，包括制定信息安全政策、明确安全管理职责、实施安全控制措施等。企业在获得 ISO27001 认证后，其客户对企业的数据安全保障能力更有信心，更愿意选择与企业合作。企业可以将 ISO27001 认证标识展示在官方网站、产品宣传资料等显著位置，向市场传递其在信息安全方面的专业性和可靠性，从而提升品牌的公信力。

（2）DSMM 数据安全能力成熟度认证

DSMM 数据安全能力成熟度认证是依据 GB/T 37988-2019《信息安全技术数据安全能力成熟度模型》标准，以组织的数据为中心，围绕数据全生命周期，从组织建设、制度流程、技术工具、人员能力四个能力维度，按照 1-5 级成熟度，评判组织的数据安全能力。通过 DSMM 认证，企业能够证明其具备成熟的数据安

全管理体系和技术能力。在申请认证过程中，企业需要对自身的数据安全能力进行全面梳理和提升，包括数据分类分级管理、数据安全防护技术应用等。企业通过DSMM认证后，可以向客户展示其在数据安全保护方面的卓越能力，增强客户对其品牌的信任。

（3）DSM数据安全管理认证

DSM数据安全管理认证是依据GB/T 41479-2022《信息安全技术网络数据处理安全要求》及相关标准规范开展的认证服务。该认证旨在规范网络运营者的网络数据处理活动，加强数据安全保护，满足国家法律法规要求，提升企业数据安全管理能力。该认证围绕数据安全管理的策略、组织架构、流程以及技术手段等多个关键要素展开评估。企业若要获取DSM认证，需构建起完备的数据安全管理策略，明确各部门和岗位在数据安全管理中的具体职责，形成清晰的组织架构。

（4）DCMM数据管理能力成熟度认证

DCMM数据管理能力成熟度认证是依据GB/T 36073-2018《数据管理能力成熟度评估模型》开展的认证服务。DCMM紧密围绕数据的全生命周期管理，科学且系统地将数据管理能力划分为8大核心能力域和28个细分能力项，全面覆盖了从战略规划层面到技术落地实施的整个流程，为企业的数据管理提供了全方位的指导框架。获得DCMM认证的企业，表明其在数据战略、数据治理、数据质量等方面达到了一定的成熟度。企业通过DCMM认证后，可以优化内部的数据管理流程，提高数据利用效率，同时也向客户展示其在数据管理方面的专业性，提升品牌的市场认可度。

（5）个人信息保护（PIP）认证

个人信息保护（PIP）认证是依据《个人信息保护法》和GB/T 35273-2020《信息安全技术个人信息安全规范》及相关标准规范开展的认证服务。该认证旨在帮助个人信息处理者规范个人信息处理活动，确保个人信息的安全与合规，提升企业在个人信息保护方面的管理水平和市场竞争力。企业在申请PIP认证时，

需要建立起完善的个人信息保护管理体系，涵盖个人信息的收集、存储、使用、共享、转让、公开披露等全生命周期的管理。通过获得 PIP 认证，企业能够向用户和市场证明其在个人信息保护方面达到了国内领先水平，对于提升企业在国内市场的品牌形象具有重要意义，特别是对于那些涉及大量个人信息处理的企业，如互联网平台企业、金融机构等，该认证可以增强用户对其个人信息保护能力的信任。

（6）GDPR（通用数据保护条例）合规认证

GDPR 是一项全面的数据保护法规，为欧盟及欧洲经济区内的个人数据收集、使用、处理和传输设定了明确的标准，被认为是目前最严格的用户隐私及数据保护法律。对于涉及欧盟用户数据的企业，遵循 GDPR 是至关重要的。GDPR 对数据保护和隐私规定了严格的要求，包括数据主体权利、数据处理原则等。企业通过确保自身的数据处理活动符合 GDPR 要求，能够展示其对用户隐私的尊重和保护能力。跨国电商企业在处理欧盟用户数据时严格遵循 GDPR，不仅避免了因违规带来的法律风险，还可以赢得欧盟用户的信任，提升品牌在国际市场上的形象。

2. 提升用户满意度，增强品牌口碑

（1）保护用户个人信息安全

数据合规建设成果中的数据安全技术措施，如加密技术、访问控制技术等，能够有效保护用户数据安全。企业应向用户清晰传达其在数据保护方面所做的努力和措施，让用户放心。例如，一家在线教育企业采用先进的加密算法保护用户的学习记录和个人信息，同时在隐私政策中详细说明数据保护措施，增强了用户对品牌的信任，提高了用户满意度。

（2）提供透明的数据使用说明

企业应向用户提供透明的数据使用说明，让用户了解企业如何使用他们的数

据。通过在产品或服务的使用过程中，及时、准确地告知用户数据的用途和处理方式，企业能够增强用户的信任感。明确告知用户应用将收集哪些数据以及如何使用这些数据，使用户在使用应用时更加安心，从而提升用户对品牌的好感度。

（3）及时响应用户诉求

当用户对数据处理或个人信息保护问题提出诉求时，企业应及时响应并妥善处理。数据合规管理体系中的客户反馈机制能够确保企业及时了解用户的需求和问题，并采取有效措施解决。对于用户关于个人信息权益的疑问和投诉，能够在规定时间内给予回复和处理，从而提高用户的满意度，维护企业品牌的良好形象。

3. 增强合作方信任，稳固品牌合作关系

（1）展示数据合规管理能力

企业在与合作方进行合作时，可以通过展示其数据合规管理体系和技术措施，证明自身具备良好的数据管理能力。在与供应商合作时，企业可以向供应商介绍其数据安全保护措施和合规政策，让供应商放心地与企业共享数据。同样，在与合作伙伴进行数据共享或合作项目时，展示数据合规能力能够增强合作方的信任，促进合作的顺利进行。

（2）遵守合作协议中的数据条款

企业应严格遵守与合作方签订的合作协议中的数据保护条款，确保数据的合法合规使用。在与第三方数据服务提供商合作时，企业应明确双方的数据权利和义务，确保数据服务提供商按照协议约定处理数据。通过遵守合作协议，企业能够树立良好的合作信誉，增强合作方对品牌的信任。

（3）共同应对数据合规挑战

在与合作方合作过程中，企业可以与合作方共同应对数据合规挑战，分享数据合规经验和最佳实践。例如，在行业数据合规标准不断更新的情况下，企业与

合作方可以共同研究和应对新的合规要求，提升双方的数据合规能力。通过这种合作，企业不仅能够增强与合作方的关系，还能在行业内树立积极合作、共同发展的品牌形象。

提升企业品牌形象是一个综合性的过程，企业可以充分利用已有的数据合规建设成果，从借助权威认证、提升用户满意度、增强合作方信任等多个方面入手。通过这些努力，企业不仅能够提升品牌的公信力、口碑和行业地位，还能在激烈的市场竞争中脱颖而出，实现可持续发展。

（三）促进数据资产管理

2025 年 1 月 6 日，国家发展改革委等部门印发了《关于完善数据流通安全治理更好促进数据要素市场化价值化的实施方案》的通知。统筹发展和安全，建立健全数据流通安全治理机制，提升数据安全治理能力，促进数据要素合规高效流通利用，释放数据价值。运用数据合规建设成果促进数据资产管理，是企业在数字经济时代实现可持续发展，寻找第二增长曲线的重要路径之一。通过确保牢数据资产合规基础、提升数据资产质量、明确数据资产权益、保障数据资产入表和促进数据产品交易等措施，企业可以充分发挥数据资产的价值，提高自身的核心竞争力。

1. 确保数据资产合规基础

数据合规管理有助于建立规范的数据资产管理流程。从数据的源头开始，对数据的产生、采集、传输、存储等过程进行严格的规范和监控，确保数据的真实性、准确性和完整性。同时，明确数据管理各环节的责任和权限，避免出现数据管理混乱、职责不清的情况。通过制定数据合规管理制度和流程，企业可以保障

数据资产管理的源头合规，为数据资产的有效利用奠定坚实的基础。

2. 提升数据资产质量

数据质量是数据资产价值的重要体现。通过数据合规建设中的数据质量管理措施，企业可以提高数据的准确性、完整性、一致性和时效性。

（1）建立质量标准

企业应制定数据质量标准，对数据质量指标进行评估和监控。通过数据清洗、校验、更新等手段，及时发现和纠正数据中的错误和不一致性，提高数据的质量和可用性。高质量的数据能够为企业的决策提供更准确的依据，帮助企业更好地把握市场机会，优化业务流程，从而提升数据资产的价值。

（2）促进数据整合

在企业的日常运营中，往往会产生大量分散在不同系统、不同部门的数据。通过对这些数据进行整合和共享，可以打破数据孤岛，实现数据的互联互通。通过建立统一的数据平台和数据共享机制，企业能够更好地挖掘数据之间的关联和价值，为企业的业务创新和发展提供支持。例如，将市场营销部门的数据与客户服务部门的数据进行整合，可以更好地了解客户需求和行为，从而制定更符合客户需求的服务方案。

3. 明确数据资产权益

数据资产确权是数据资产管理的重要环节。在数据合规建设成果的基础上，企业可以结合业务场景规范数据资产确权方式，明确数据资产的权利归属。

（1）落实产权机制

企业通过明确数据资产的产权归属，确定数据资源的持有权、使用权和经营权等权利主体，避免因数据产权不清晰而引发的纠纷和争议。通过数据产权登记

机制，企业可以将数据资产的产权信息进行登记和公示，为数据资产的交易、出资入股、质押融资等提供合法依据，保障企业的数据资产权益。

（2）加强权益保护

在数据资产的开发利用过程中，涉及到多个主体的权益，如数据提供者、数据处理者、数据使用者等。企业应建立健全数据权益保护机制，明确各主体的权利和义务，保障各方的合法权益。通过签订数据使用协议、保密协议等法律文件，规范数据的使用范围和方式，防止数据被滥用或泄露，保护数据提供者的隐私和商业秘密。同时，对于数据处理者和使用者，也要明确其在数据处理和使用过程中的权利和责任，确保其能够合法、合规地使用数据资产，实现数据资产的价值最大化。

4. 保障数据资产入表

数据合规建设成果为数据资产入表提供了有力的支持。合规的数据资产来源和处理过程是数据资产入表的前提条件。企业需要确保数据资产的合法合规性，才能将其纳入财务报表。

（1）规范会计处理

2023 年 8 月 1 日，财政部下发了《企业数据资源相关会计处理暂行规定》，为企业数据资源的会计处理提供了明确的规范。该规定已于 2024 年 1 月 1 日起施行，企业可以按照规定对符合条件的数据资源进行准确的会计确认、计量和报告。企业可以将数据资源确认为无形资产或存货等资产类别，并在资产负债表中进行列示，如实反映企业的数据资产价值。这不仅有助于企业准确评估自身的资产状况，还能为企业的投资者、债权人等利益相关者提供更准确的财务信息，增强企业的市场透明度和公信力。

（2）提升决策支持

数据资产入表能够为企业的决策提供更有力的支持。通过对数据资产的价值进行量化和评估，企业可以更好地了解数据资产对企业财务状况和经营成果的影响，从而在投资决策、战略规划等方面做出更科学、合理的决策。例如，在考虑是否投入资源进行数据资产的开发和利用时，企业可以通过分析数据资产的预期收益和成本，评估其对企业未来利润的贡献，从而决定是否进行投资。同时，数据资产入表也有助于企业在并购、重组等资本运作过程中，准确评估目标企业的数据资产价值，避免因数据资产价值评估不准确而导致的交易风险。

5. 促进数据产品交易

数据资产产品化是企业实现数据价值增值的重要途径。在数据合规建设的基础上，企业可以通过对数据的深度分析和挖掘，开发出基于数据的新产品和新服务，满足市场的个性化需求。数据产品交易是数据要素市场化的关键环节，数据质量是基础，数据确权、定价是关键，数据安全和合规有序的交易环境是保障。数据合规管理为数据资产的产品化和市场化交易提供了必要的保障。在数据合规建设成果的基础上，企业可以通过建立规范的数据产品生产和管理机制，将数据资产进行包装和加工，转化为具有市场价值的数据产品，并在合法合规的前提下进行交易。这不仅能够为企业带来额外的收入来源，还能促进数据要素的流通和共享，推动数字经济的发展。

合规创造信任，信任驱动价值。企业需将数据合规建设成果转化为资产管理各环节的具体措施：从源头确保数据资产合法合规，依托合规品牌拓展市场，最终构建可信赖的数据市场生态。在实践中，企业应避免将合规视为成本，而应将其作为数字化时代的核心竞争力——当合规成为数据交易的“通行证”和“护城河”，数据价值的释放将更具持续性和扩展性。未来，随着数据要素市场的成熟，合规能力不仅是企业的必备资质，更是数据产品的核心卖点，唯有持续深耕合规

建设，才能在数字经济浪潮中占据先机。

（四）推动新兴技术应用

在数字技术加速迭代的时代，人工智能、区块链、物联网、隐私计算等新兴技术正成为企业创新发展的核心驱动力。然而，新兴技术的应用往往伴随数据收集范围扩大、处理复杂度提升等合规风险。企业完成数据合规管理体系建设后，需将合规成果深度融入新兴技术应用场景，在释放技术红利的同时守住安全合规底线。

1. 以合规框架护航新兴技术应用合法性

合规框架是企业开展新兴技术应用的基石，它为技术应用提供了明确的法律依据和行为准则，确保技术应用在合法合规的轨道上运行。

（1）人工智能技术应用

在人工智能领域，算法的应用可能涉及到数据的采集、处理和使用，若算法存在偏见或歧视，可能会侵犯用户的合法权益。因此，企业需要建立健全的合规框架，对算法的设计、开发和应用进行严格规范。例如，明确算法的数据来源和使用目的，确保数据的合法性和合规性；对算法的运行过程进行监控和审计，及时发现和纠正算法中的偏差和错误。

（2）区块链技术应用

在区块链技术应用中，智能合约的执行需要依赖大量的数据，这些数据的真实性和可靠性直接影响到智能合约的有效性。为了确保智能合约的合法合规，企业需要建立完善的合规框架，对智能合约的制定、执行和管理进行规范。比如，明确智能合约的法律地位和法律效力，确保智能合约符合法律法规的要求；对智

能合约的数据输入和输出进行审核，防止数据造假和篡改。通过建立合规框架，企业能够为新兴技术应用提供坚实的法律保障，确保技术应用的合法性和合规性。

（3）物联网技术应用

在物联网领域，设备之间的互联互通会产生大量的数据，这些数据涉及到用户的隐私和安全。为了保护用户的隐私和安全，企业可以采用加密技术，对数据进行加密处理，防止数据在传输和存储过程中被窃取或篡改。同时，企业还可以采用访问控制技术，对设备的访问权限进行管理，确保只有授权的设备才能访问敏感数据。

（4）隐私计算技术应用

在隐私计算领域，如何在保护数据隐私的前提下实现数据的共享和分析，是一个亟待解决的问题。为了破解这一难题，企业可以采用多方安全计算、联邦学习等隐私计算技术。这些技术能够在不泄露原始数据的前提下，实现数据的联合分析和建模，为企业提供了一种安全、合规的数据共享和分析解决方案。例如，在医疗领域，通过隐私计算技术，不同医疗机构之间可以在保护患者隐私的前提下，共享医疗数据，开展联合研究和诊断，提高医疗水平。

2. 以合规信任体系提升新兴技术接受度

在新兴技术应用过程中，用户对技术的信任是技术成功应用的关键。为了提升用户对新兴技术的接受度，企业可以通过数据合规建设成果加强信任体系的建立。

（1）合规能力可视化展示

企业通过加强新技术应用中的数据安全和隐私保护，确保用户的数据得到妥善保护。通过合规能力可视化展示向用户证明其对数据安全和隐私保护的重视，增强用户对技术的信任。例如，在新兴技术产品官网设置“合规中心”，公开技

术应用的合规证书、数据处理流程示意图；发布《新兴技术合规白皮书》，详细说明技术实现中的数据分类分级方法、隐私保护技术方案等；提供《新兴技术合规审计报告》，通过客观公正的审计结果证明企业在新兴技术应用方面的合规能力。

（2）提高技术的透明度和可解释性

在人工智能领域，算法的黑盒性质使得用户难以理解算法的决策过程和结果，从而降低了用户对算法的信任。为了提高算法的透明度和可解释性，企业可以采用可解释性算法，对算法的决策过程进行可视化展示，让用户能够理解算法的工作原理和决策依据。同时，企业还可以建立算法解释机制，当用户对算法的决策结果提出质疑时，能够及时提供合理的解释，增强用户对算法的信任。

3. 以动态合规机制应对新兴技术合规挑战

新兴技术快速发展的同时，合规要求也在不断改进。为了应对新兴技术带来的合规挑战，企业需要建立动态的合规管理机制。

（1）跟踪和研究合规趋势

企业要加强对新兴技术发展趋势的，及时了解技术发展带来的合规风险和挑战。通过关注行业动态、参与技术标准制定等方式，企业能够提前做好应对准备，及时调整合规策略和措施。

（2）建立合规风险评估和预警机制

企业应定期对新兴技术应用中的合规风险进行评估，及时发现潜在的合规风险，并采取相应的措施进行防范和化解。同时，企业还可以建立合规风险预警系统，对可能出现的合规风险进行实时监测和预警，及时发出预警信号，提醒企业采取措施进行应对。

（3）加强沟通与合作

企业要加强与监管部门、行业协会等的沟通与合作。及时了解监管政策的变化，积极参与行业标准的制定和修订，与监管部门和行业协会保持密切的沟通与合作，共同推动新兴技术的合规发展。

推动新兴技术应用的核心在于实现“技术创新”与“安全合规”的平衡。企业需将数据合规建设成果转化为新兴技术全生命周期的管控能力：从研发阶段的合规前置审查，到应用阶段的技术风险化解，再到市场层面的合规信任构建，最终形成技术驱动与合规保障的良性循环。在实践中，企业应避免将合规视为技术创新的“枷锁”，而是作为技术价值释放的“护航器”——当新兴技术的每一次迭代都建立在合规基石之上，其创新成果才能获得市场的广泛认可和持续信赖。未来，随着技术与合规的深度融合，合规能力将成为企业新兴技术应用的核心竞争力。

附录一：专业术语释义

序号	术语	释义
1	数据	是指任何以电子或者其他方式对信息的记录。（《中华人民共和国数据安全法》第三条）
2	数据处理	包括数据的收集、存储、使用、加工、传输、提供、公开等。（《（中华人民共和国数据安全法》第三条）
3	数据安全	是指通过采取必要措施，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。（《中华人民共和国数据安全法》第三条）
4	数据处理者	在数据处理活动中自主决定处理目的、处理方式的组织、个人。（GB/T 43697-2024《数据安全技术数据分类分级规则》3.术语与定义）
5	网络数据	是指通过网络处理和产生的各种电子数据。（《网络数据安全管理条例》第六十二条）
6	数据脱敏	对某些敏感信息通过一定规则进行数据的变形，实现敏感隐私数据可靠保护。（GB/T 37988—2019《信息安全技术数据安全能力成熟度模型》3.术语和定义）
7	重要数据	是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。（《网络数据安全管理条例》第六十二条）
8	核心数据	对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。（GB/T 43697—2024《数据安全技术数据分类分级规则》3.术语与定义）

9	一般数据	核心数据、重要数据之外的其他数据。（GB/T 43697—2024《数据安全技术数据分类分级规则》3.术语与定义）
10	数据安全风险	数据安全事件的发生可能性及其对国家安全、公共利益或者组织、个人合法权益造成的损害。（GB/T45577—2025《数据安全技术数据安全风险评估方法》3.术语和定义）
11	数据安全风险评估	对数据和数据处理活动安全进行风险识别、风险分析和风险评价的整个过程。（GB/T45577—2025《数据安全技术数据安全风险评估方法》3.术语和定义）
12	个人信息	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。（《中华人民共和国个人信息保护法》第四条）
13	个人信息主体	个人信息已识别或者可识别的自然人。（GB/T 41479—2022《信息安全技术网络数据处理安全要求》3.术语与定义）
14	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。（《中华人民共和国个人信息保护法》第四条）
15	个人信息处理者	是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。（《中华人民共和国个人信息保护法》第七十三条第一款）
16	敏感个人信息	敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。（《中华人民共和国个人信息保护法》第二十八条）
17	境外接收方	是指在中华人民共和国境外自个人信息处理者处接收个人信息的组织、个人。（《个人信息出境标准合同备案指南（第一版）》）

18	个人信息保护影响评估	个人信息保护影响评估由个人信息安全影响评估演变而来，是针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。（GB/T 35273—2020《信息安全标准个人信息安全规范》3.术语和定义）
19	匿名化	是指个人信息经过处理无法识别特定自然人且不能复原的过程。（《中华人民共和国个人信息保护法》第七十三条）
20	去标识化	是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。（《中华人民共和国个人信息保护法》第七十三条第三款）
21	自动化决策	是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。（《中华人民共和国个人信息保护法》第七十三条第二款）
22	个人信息共享	个人信息控制者向其他控制者提供个人信息，且双方分别对个人信息拥有独立控制权的过程。（GB/T 35273—2020《信息安全标准个人信息安全规范》3.术语和定义）
23	个人信息转让	将个人信息控制权由一个控制者向另一个控制者转移的过程。（GB/T 35273—2020《信息安全标准个人信息安全规范》3.术语和定义）
24	公开披露	向社会或不特定人群发布信息的行为。（GB/T 35273—2020《信息安全标准个人信息安全规范》3.术语和定义）
25	委托处理	是指网络数据处理者委托个人、组织按照约定的目的和方式开展的网络数据处理活动。（《网络数据安全管理条例》第六十二条）
26	共同处理	是指两个以上的网络数据处理者共同决定网络数据的处理目的和处理方式的网络数据处理活动。（《网络数据安全管理条例》第六十二条）

27	单独同意	是指个人针对其个人信息进行特定处理而专门作出具体、明确的同意。（《网络数据安全管理条例》第六十二条）
28	大型网络平台	是指注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。（《网络数据安全管理条例》第六十二条）
29	关键信息基础设施	是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。(《关键信息基础设施安全保护条例》第二条）

附录二：法律法规及标准索引

（一）已生效文件

序号	文件名称	颁布时间	实施时间	颁布机构
法律				
1	《中华人民共和国反垄断法》	2007 年 8 月 30 日	2008 年 8 月 1 日	全国人民代表大会常务委员会
2	《中华人民共和国网络安全法》	2016 年 11 月 7 日	2017 年 6 月 1 日	全国人民代表大会常务委员会
3	《中华人民共和国反不正当竞争法》	2017 年 11 月 4 日	2018 年 1 月 1 日	全国人民代表大会常务委员会
4	《中华人民共和国民法典》	2020 年 5 月 28 日	2021 年 1 月 1 日	全国人民代表大会
5	《中华人民共和国行政处罚法》	2021 年 1 月 22 日	2021 年 7 月 15 日	全国人民代表大会常务委员会
6	《中华人民共和国数据安全法》	2021 年 6 月 10 日	2021 年 9 月 1 日	全国人民代表大会常务委员会

7	《中华人民共和国个人信息保护法》	2021 年 8 月 20 日	2021 年 11 月 1 日	全国人民代表大会常务委员会
8	《中华人民共和国刑法》	2023 年 12 月 29 日	2024 年 3 月 1 日	全国人民代表大会
行政法规				
9	《计算机信息系统安全保护条例》	1994 年 2 月 18 日	1994 年 2 月 18 日	国务院
10	《关键信息基础设施安全保护条例》	2021 年 7 月 30 日	2021 年 9 月 1 日	国务院
11	《未成年人网络保护条例》	2023 年 10 月 16 日	2024 年 1 月 1 日	国务院
12	《网络数据安全管理条例》	2024 年 9 月 24 日	2025 年 1 月 1 日	国务院
司法解释				
13	《关于适用〈反不正当竞争法〉若干问题的解释》	2022 年 3 月 16 日	2022 年 3 月 20 日	最高人民法院
部门规章及规范性文件				
14	《信息安全等级保护管理办法》	2007 年 6 月 22 日	2007 年 6 月 22 日	公安部、国家保密局、国家密码

				管理局、国务院信息化工作办公室
15	《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》	2018 年 11 月 15 日	2018 年 11 月 30 日	国家互联网信息办公室
16	《网络信息内容生态治理规定》	2019 年 12 月 15 日	2020 年 3 月 1 日	国家互联网信息办公室
17	《深圳经济特区数据条例》	2021 年 7 月 6 日	2022 年 1 月 1 日	深圳市第七届人民代表大会常务委员会
18	《汽车数据安全管理若干规定（试行）》	2021 年 8 月 16 日	2021 年 10 月 1 日	国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部
19	《互联网信息服务算法推荐管理规定》	2021 年 12 月 31 日	2022 年 3 月 1 日	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
20	《数据出境安全评估办法》	2022 年 7 月 7 日	2022 年 9 月 1 日	国家互联网信息办公室
21	《互联网信息服务深度合成管理规定》	2022 年 11 月 25 日	2023 年 1 月 10 日	国家互联网信息办公室、工业和信息化部、公安部
22	《工业和信息化领域数据安全管理办法（试行）》	2022 年 12 月 8 日	2023 年 1 月 1 日	工业和信息化部
23	《个人信息出境标准合同办法》	2023 年 2 月 24 日	2023 年 6 月 1 日	国家互联网信息办公室
24	《个人信息保护认证实施规则》	2023 年 6 月 20 日	2023 年 6 月 20 日	国家市场监督管理总局、国家互联网信息办公室
25	《生成式人工智能服务管理暂行办法》	2023 年 7 月 13 日	2023 年 8 月 15 日	国家互联网信息办公室、国家发展和改革委员会、教育部、科学技术部、工业和信息化部、公

				安部、国家广播电视总局
26	《企业数据资源相关会计处理暂行规定》	2023 年 8 月 1 日	2024 年 1 月 1 日	财政部
27	《科技伦理审查办法（试行）》	2023 年 9 月 11 日	2023 年 12 月 1 日	科学技术部、教育部、工业和信息化部、农业农村部、国家卫生健康委员会、中国科学院、中国社会科学院、中国工程院、中国科学技术协会、中央军事委员会科学技术委员会
28	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	2023 年 12 月 13 日	2023 年 12 月 13 日	国家互联网信息办公室、香港特别行政区政府创新科技及工业局

29	《促进和规范数据跨境流动规定》	2024 年 3 月 22 日	2024 年 3 月 22 日	国家互联网信息办公室
30	《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》	2024 年 9 月 10 日	2024 年 9 月 10 日	国家互联网信息办公室、澳门特别行政区政府经济及科技发展局、澳门特别行政区政府个人资料保护局
31	《个人信息保护合规审计管理办法》	2025 年 2 月 14 日	2025 年 5 月 1 日	国家互联网信息办公室
32	《人工智能生成合成内容标识办法》	2025 年 3 月 14 日	2025 年 9 月 1 日	国家互联网信息办公室、工业和信息化部、公安部、国家广播电视总局
国家标准与行业指南				
33	GB/T 36073–2018《数据管理能力成熟度评估模型》	2018 年 3 月 15 日	2018 年 10 月 1 日	全国信息技术标准化技术委员会

34	GB/T 28449-2018《信息安全技术网络安全等级保护测评过程指南》	2018年12月28日	2019年7月1日	全国信息安全标准化技术委员会
35	GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》	2019年5月10日	2019年12月1日	全国信息安全标准化技术委员会
36	GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》	2019年5月10日	2019年12月1日	全国信息安全标准化技术委员会
37	GB/T37988-2019《信息安全技术数据安全能力成熟度模型》	2019年8月30日	2020年3月1日	全国信息安全标准化技术委员会
38	GB/T 25058-2019《信息安全技术网络安全等级保护实施指南》	2019年8月30日	2020年3月1日	全国信息安全标准化技术委员会
39	GB/T 35273-2020	2020年3月6日	2020年10月1日	全国信息安全标准

	《信息安全技术个人信息安全规范》			化技术委员会
40	GB/T 39335–2020《信息安全技术个人信息安全影响评估指南》	2020 年 11 月 19 日	2021 年 6 月 1 日	全国信息安全标准化技术委员会
41	国反垄发〔2021〕1 号《关于平台经济领域的反垄断指南》	2021 年 2 月 7 日	2021 年 2 月 7 日	国务院反垄断委员会
42	GB/T 41479–2022《信息安全技术网络数据处理安全要求》	2022 年 4 月 15 日	2022 年 11 月 1 日	全国信息安全标准化技术委员会
43	GB/T 41867–2022《信息技术人工智能术语》	2022 年 10 月 12 日	2023 年 5 月 1 日	全国信息技术标准化技术委员会
44	GB/T 42888–2023《信息安全技术机器学习算法安全评估规范》	2023 年 8 月 6 日	2024 年 3 月 1 日	全国信息安全标准化技术委员会
45	TC260–PG–20244A《网络安全标准实践指南	2024 年 9 月 14 日	2024 年 9 月 14 日	全国网络安全标准化技术委

	—敏感个人信息识别指南》			员会
46	GB/T 44588—2024《数据安全技术互联网平台及产品服务个人信息处理规则》	2024 年 9 月 29 日	2025 年 4 月 1 日	全国网络安全标准化技术委员会
47	GB 45438—2025《网络安全技术人工智能生成合成内容标识方法》	2025 年 2 月 28 日	2025 年 9 月 1 日	全国网络安全标准化技术委员会
48	GB/T45404—2025《数据安全技术大型互联网企业内设个人信息保护监督机构要求》	2025 年 3 月 28 日	2025 年 10 月 1 日	全国网络安全标准化技术委员会
49	GB/T45392—2025《数据安全技术基于个人信息的自动化决策安全要求》	2025 年 3 月 28 日	2025 年 10 月 1 日	全国网络安全标准化技术委员会
50	GB/T 45654—2025《网络安全技术生成式人工智能服务安全基本要求》	2025 年 4 月 25 日	2025 年 11 月 1 日	全国网络安全标准化技术委员会

51	GB/T 45674—2025《网络安全技术生成式人工智能数据标注安全规范》	2025 年 4 月 25 日	2025 年 11 月 1 日	全国网络安全标准化技术委员会
52	GB/T 45652—2025《网络安全技术生成式人工智能预训练和优化训练数据安全规范》	2025 年 4 月 25 日	2025 年 11 月 1 日	全国网络安全标准化技术委员会
53	GB/T45577—2025《数据安全技术数据安全风险评估方法》	2025 年 4 月 25 日	2025 年 11 月 1 日	全国网络安全标准化技术委员会
54	GB/T 45574—2025《数据安全技术敏感个人信息处理安全要求》	2025 年 4 月 25 日	2025 年 11 月 1 日	全国网络安全标准化技术委员会

（二）未生效文件

序号	文件名称	发布时间	发布机构
行政法规			
1	《网络安全等级保护条例（征求意见稿）》	2018 年 6 月 27 日	公安部
部门规章及规范性文件			
2	《个人信息出境个人信息保护认证办法（征求意见稿）》	2025 年 1 月 6 日	国家互联网信息办公室
国家标准与行业指南			
3	《信息安全技术重要数据识别指南（征求意见稿）》	2022 年 1 月 13 日	全国信息安全标准化技术委员会
4	《数据安全技术个人信息保护合规审计要求（征求意见稿）》	2024 年 7 月 12 日	全国网络安全标准化技术委员会
5	《网络安全标准实践指南—个人信息保护合规审计要求（征求意见稿）》	2025 年 4 月 28 日	全国网络安全标准化技术委员会

参编单位与人员

主编单位：

中共深圳市龙华区委宣传部

参编单位：

深圳市常行科技有限公司

泰和泰（深圳）律师事务所

广和律师事务所

北京安华金和科技有限公司

全知科技（杭州）有限责任公司

深圳市捷顺科技实业股份有限公司

深圳汉王友基科技有限公司

深圳市华宝新能源股份有限公司

总 策 划： 黄立敏

总　　编： 吴　江　张　煦

编　　委： 范　超　赵振动　刘大亮　张　巍　肖赛尔　吴港澳

参编人员： 万　硕　李德尧　高健坤　姜聪杰　朱小良　黄启友　卢茂生

吴庆飞　郭志鹏　龙　军　郭　义　庄　严　吴华超　冯志文

肖　健　龚顺东　郭　辉　孙剑浩　郑家涛　肖立洁