吴中区企业数据合规指引

目 录

第一章 总则

第一条 指引目的

本指引制定目的为引导企业加强数据合规管理，规范数据处理活动，保护个人信息，保障企业数据安全，促进企业数据合规利用，为企业发展保驾护航。

第二条 法律依据

根据《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国网络安全法》、《苏州市数据条例》等法律、法规，制定本指引。

第三条 适用范围

吴中区各类企业进行数据处理活动均可参照本指引开展数据合规管理。本指引不具有强制性，法律、法规及有关国家、行业标准对数据合规另有专门规定的，从其规定。

第四条 基本原则

企业开展数据处理活动应当遵循合法、正当、必要和诚信原则，不得从事危害国家安全、公共利益的数据处理活动，也不得损害自然人、法人、非法人组织的合法权益。

第二章 数据合规管理体系

第五条 一般要求

企业开展数据处理活动应当依照法律、法规的规定，健全企业数据合规专门机构与运行机制，明确各机构和员工的职责和权限，组织数据合规培训和企业合规文化建设，以实现有效防控数据处理活动中法律风险的目的。

第六条　数据合规责任人的职责

数据合规管理的负责人一般由企业的法定代表人或者主要负责人担任，应当承担以下职责：

（一）根据企业的实际情况和行业特点，制定合适的数据合规战略，明确数据合规的目标、范围和实施计划；

（二）设立专门的数据合规部门，负责企业数据合规管理事务，指导数据处理活动；

（三）促进企业内部各部门之间的协作与沟通，使得数据合规管理工作得以顺利实施。

（四）为企业数据合规提供必要的资源保障，包括人力、物力、财力等，保障企业的合规管理体系有效运行；

（五）明确合规管理部门和人员的职责分工，并保障各部门和人员具备履职的能力和权限。同时制定相应的追责机制，促使数据合规政策的落实；

（六）建立数据违规行为的举报和惩处机制；

（七）听取数据合规管理工作汇报，指导、监督、评价数据合规管理工作；

（八）倡导企业内部形成数据合规的习惯和氛围,将员工的合规理念转变为合规行为，培育企业数据合规文化。

第七条 数据合规部门的职责

有条件的企业应当设立专门的数据合规部门；无必要设立专门数据合规部门的企业，可适当配备数据合规专员，与公司法务共同承担数据合规管理的职能，应当承担以下职责：

（一）根据企业的业务需求以及法律、法规、强制性标准的要求，制定数据合规管理的制度、政策、年度工作计划等，并推动贯彻落实；

（二）定期对企业数据处理活动进行合规审查，评估数据处理活动中的法律风险，确保企业业务运营的合规；

（三）跨部门协作与沟通，推动数据合规工作在各业务领域的落实；

（四）组织数据合规培训和宣传活动，并受理业务部门和职能部门的合规咨询，提高员工对数据合规的意识，使得员工在业务操作中遵守数据合规要求；

（五）定期向数据合规负责人汇报数据合规工作情况，对合规风险和问题提出改进措施，为企业数据合规管理提供决策支持；

（六）密切关注国家法律、法规、行业政策和标准动态，及时调整和完善企业数据合规管理制度，促使企业数据合规管理满足最新合规要求；

（七）建立健全数据安全应急机制，应对数据安全突发事件，保障企业合法权益；

（八）受理数据处理违规投诉、举报，提出分类处置意见，组织或者参与对违规行为的调查；

（九）协助完成数据合规负责人交办的其他数据合规相关工作。

第八条 数据合规职能和业务部门的职责

企业职能和业务部门处在数据处理活动的前端，负责本部门业务范围内的数据合规工作，承担以下职责：

（一）根据数据合规部门制定的合规制度、政策，明确本部门数据合规工作的实施细则，使得本部门业务活动符合数据合规要求；

（二）参与合规制度、政策的制定，提供业务需求和实际应用场景，增强数据合规制度、政策的可行性和适用性；

（三）加强数据安全防护措施，包括加密、访问控制、防火墙等技术手段，以保障数据的安全性；

（四）与其他部门保持紧密合作，共同推进企业数据合规工作的顺利展开；

（五）在发生数据安全事件时要迅速响应，向数据合规部门和数据合规负责人汇报，并配合进行应急处置。

第九条 个人信息保护负责人

企业处理数据涉及的个人信息达到国家网信部门规定数量的，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。

个人信息保护负责人承担以下职责:

（一）根据法律、法规和企业的合规制度，制定相关的个人信息保护政策和措施，确保企业在处理个人信息时符合合规要求，并督促相关政策和措施有效落实；

（二）定期组织个人信息保护相关的培训和宣传活动，提高员工对个人信息保护的认识和重视；

（三）负责接收和处理与个人信息保护相关的投诉和举报，及时采取措施解决存在的问题；

（四）定期对企业个人信息处理活动进行个人信息安全影响评估，并根据评估结果进行整改；

（五）在发生涉及个人信息的紧急事件时，需要立即采取措施，保障个人信息的安全，并按照规定报告相关监管部门。企业应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

第十条 员工的数据合规义务

为督促企业员工在业务操作中遵守数据合规要求，企业应做到如下要求：

（一）在招聘过程中，应将遵守数据合规要求和履行数据合规义务作为人员聘用条件；

（二）在数据合规管理制度中明确员工的数据合规义务，包括但不限于数据收集、存储、处理和传输等环节；

（三）对数据分析、系统搭建、安全保障等关键岗位的员工，应当进行必要的背景调查，了解其民事涉诉、行政处罚、刑事犯罪记录、诚信和征信状况等，以确保关键岗位员工具备较高的道德品质和合规意识；

（四）企业应以签署合规承诺书、保密协议等方式明确员工应遵守的数据合规要求和合规义务；

（五）数据分析、系统搭建、安全保障等关键岗位的员工离岗、离职后，企业需执行离岗、离职交接、审计、脱密等措施，保证离岗、离职员工无法访问企业数据。

第十一条 数据合规的奖励机制

企业在数据合规管理中，对员工实施合理的激励措施，有助于提高员工参与数据合规工作的主动性和自觉性。企业应当将员工在数据合规中的表现纳入物质奖励、内部表彰、职务晋升等考核条件之中。

第十二条　投诉、举报和整改机制

企业应设立专门的举报和投诉渠道，及时发现并纠正数据违规行为，同时要对举报和投诉人的身份和信息予以保密。数据合规部门收到投诉、举报后，应及时启动调查，调查小组应具备专业的数据合规知识和技能，能够准确判断被投诉、举报的事项是否涉及数据违规。对于确实存在数据违规情况的，企业应采取相应的处理和整改措施，并对处理和整改结果进行反馈和公示。

第三章 数据合规管理制度

第十三条　数据分类分级制度

企业应重视数据资产的管理和保护，对数据资产进行全面梳理，并对数据进行分类分级，应做到如下要求：

（一）确定数据分类分级目标：企业应明确数据分类分级的目的，以确保制定的数据分类分级制度符合企业实际需求；

（二）制定数据分类标准：企业应根据数据的业务属性、敏感程度等因素，制定统一的数据分类标准。分类标准应具有可扩展性，以便随着企业业务的发展

进行调整；

（三）设定数据分级标准：企业应根据数据的重要程度、敏感程度和泄露可能造成的影响等因素，设定合理的数据分级标准，进一步划分为核心数据、重要数据和一般数据等级别，以满足不同数据的安全需求；

（四）数据分类分级实施：企业应将制定的数据分类分级标准应用于实际数据管理过程中，企业需确保员工在访问和处理不同类别、级别数据时，遵循权限控制、数据加密、访问日志记录等相应的操作规范；

（五）优化数据分类分级制度：企业应定期对数据分类分级制度进行审查和优化，以适应企业发展和市场变化的需要。

第十四条　风险评估机制

企业应当建立数据合规风险评估机制，每年进行不少于一次的数据合规风险评估工作，对数据合规制度、数据处理流程、数据安全措施、数据预警与应对机制等方面进行全面审查，分析潜在的风险点、合规隐患、安全漏洞，在评估过程中，重点识别数据处理活动中可能出现的合规风险，如数据泄露、不当收集、不合理使用等，以及可能造成的后果，并形成书面评估报告。企业根据风险评估结果，制定相应的风险应对策略。评估报告中涉及重要数据、核心数据的，应当向相关主管部门和监管部门报送评估报告。

第十五条　安全技术保护措施

企业在完成数据分类分级并形成数据资源目录后，针对不同种类的数据、不同级别的数据，构建相应的技术保护体系，要采取与数据种类、级别相匹配的数据备份、数据加密、访问控制、设立防护墙、建立入侵测试和防御系统等数据保护手段，并强化对数据存储环境、数据传输过程、数据访问接口等网络环境的安全防御，并将安全技术保护贯彻到数据全生命周期。

处理重要数据的系统应满足三级以上网络安全等级保护和关键信息基础设施安全保护的要求，应当按照相关规定从严保护处理核心数据的系统。

第十六条　安全应急响应机制

企业应当制定数据安全应急预案，包括明确职责、安全事件分级、响应流程等，以应对数据安全风险：

（一）建立数据安全应急管理体系：明确组织架构、人员职责和沟通协作机制，确保在数据安全事件发生时，各相关部门能够快速响应、协同处理；

（二）数据安全事件分级：根据数据影响范围、危害程度等因素，将数据安全事件分为不同等级，并根据不同等级制定相应的应急处置措施；

（三）数据安全事件响应流程：企业在面临安全威胁时，采取一系列有序、高效的应对措施，及时发现、通报并响应数据安全事件：

1、发现安全事件：通过监控设备、安全审计工具等方式，对系统、网络进行实时监控，及时发现可能存在的安全隐患；

2、通报安全事件：在发现安全事件后，迅速向相关负责人、部门或员工通报，确保相关人员了解安全状况；

3、分析安全事件：对安全事件进行深入分析，了解事件原因、影响范围、潜在损失等，明确对应的安全事件等级；

4、执行应急处置措施：根据安全事件等级，将制定好的响应策略付诸实践，包括对受损系统、数据进行修复和恢复等；

5、评估响应效果：在执行响应措施后，对安全事件的影响进行评估，检查响应措施是否有效；

6、定期演练与完善：定期组织安全事件应急演练，检验安全事件发现、通报和响应流程的执行情况，不断优化数据安全事件处置措施，提高实际应对能力。

第十七条　数据安全审查申报机制

企业应当根据数据规模、涉及领域等因素，制定相应的审查标准和申报机制，并积极主动审查数据处理活动是否可能涉及国家安全、经济运行、社会稳定、公共健康和安全，符合法律、法规规定条件的，应当按照有关规定，申报数据安全

审查。

企业数据安全审查申报机制的制定需细化审查标准和流程，明确审查范围、审查主体、审查程序和审查时限等。此外，审查标准应具有一定的灵活性，以便应对数据安全形势的不断变化。

第十八条　数据合规培训制度

企业通过组织各部门员工开展学习数据保护法律、法规、标准以及数据合规管理的具体要求和方法等培训活动，旨在提高员工的数据合规意识和能力，保障企业数据安全，有效规避数据处理活动中蕴含的法律风险。

第四章 数据全生命周期合规

第十九条　数据收集

（一）以自动化工具获取公开数据的合规要求

企业采用爬虫技术等自动化工具收集数据的，应当确保收集方式合法、正当，遵守法律、法规、行业自律公约、对象网站的协议及规则，评估网络服务性能及可能带来的影响，避免干扰网络服务的正常功能或妨碍计算机信息系统正常运行。

企业使用自动化工具收集公开数据的，应当符合以下要求：

1、不得以不正当竞争为目的获取数据；

2、不得违法侵入涉密网站和计算机信息系统获取数据；

3、不得以非法获取内部访问、操作权限等方式，未经授权或超越授权范围获取数据；

4、不得干扰被访问网站的正常运营或者妨碍计算机信息系统正常运行；

5、不得以技术破解方式突破网站、计算机信息系统为保护数据而设置的技术保护措施；

6、法律、法规规定的其他要求。

（二）以购买方式获取数据的合规要求

企业通过购买方式获取数据的，应对数据提供方的资质以及获取和持有数据的合规性进行必要审查，要求其作出数据来源、数据类型、数据范围、数据安全等合法性承诺并提供必要证明。对于以购买方式获取的数据，企业应当承担与以直接方式收集的数据同等的安全保护责任与合规义务。

（三）以交换、共享方式获取数据的合规要求

1、企业在进行数据交换和共享前，应明确数据交换的目的、范围和涉及的主体。确定数据交换的背景和动机，明确数据共享的对象、类型和规模，以及界定数据交换所涉及的业务领域和部门；

2、企业应签订书面的数据交换和共享协议。协议内容应包括数据类型、数据用途、数据存储期限、数据安全措施、数据隐私保护、数据合规审查等方面的要求；

3、企业在数据交换和共享过程中，应采取充分的数据安全保护措施，对数据进行加密、脱敏、去标识化等处理，设置访问权限，确保数据在交换和共享过程中的安全；

4、对数据交换和共享活动，企业应建立定期审查机制，对数据交换和共享活动进行全面、持续的监督，及时发现问题并整改。此外，企业还应加强对数据交换和共享过程中涉及的敏感数据、特殊数据的管理。

（四）在提供产品、服务过程中获取数据的合规要求

1、企业在产品或服务的基本业务功能开启前（如个人初始安装、首次使用、注册账号等情形），以链接等方式展示个人信息保护政策等处理规则时，应以增强告知（如设置专门界面或单独步骤）的方式主动向个人告知其中的关键规则，包括个人信息保护政策的章节结构（点击后可直接访问对应内容），基本业务功能所必需的个人信息种类，收集方式、目的等，以及处理个人信息主体询问、投诉的联系方式；在收集个人信息时应遵循最小范围、必要原则，仅收集与实现产品或服务的业务功能直接相关的信息；

2、个人信息保护政策要单独成文，而不是作为用户协议、用户说明等文件

的附属部分；个人信息保护政策要易于访问，进入 App 主功能界面后，通过 4 次以内的点击，能够访问到个人信息保护政策，且链接位置突出、无遮挡；个人信息保护政策的内容要易于阅读，文本文字显示方式（字号、颜色、行间距等）不会造成阅读困难，如文字过小过密、颜色过淡、模糊不清；个人信息保护政策的内容要易于理解，不应使用晦涩难懂、冗长繁琐等用户难以理解的文字，如使用大量专业术语等；

3、企业在开发新型业务功能或提升服务体验时，超出必要范围收集个人信息应再次征得个人明示同意。不得因个人不同意提供非必要个人信息而拒绝提供基本功能或服务；

4、企业使用收集到的数据时，需事先获得相关数据主体的授权同意，取得同意的范围不得超出所告知的内容；

5、当产品或服务提供多项需收集个人信息的业务功能的，企业不得采用捆绑方式强迫个人一次性同意多项业务功能可能收集的个人信息或多个处理活动；个人拒绝同意时，不影响与该个人信息无关的业务功能的正常使用。

（五）接受第三方委托处理数据的合规要求

企业接受第三方委托处理个人信息的，应当确保提供方已向个人告知接受方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并按照法律、法规的规定征得个人单独同意。

企业接受第三方委托处理数据的，还应当符合以下要求：

1、签订数据委托处理协议：在接受第三方数据前，双方需签订书面协议，明确数据来源、用途、保密要求、双方权利义务等相关事项，协议应包含合规性承诺和违约责任条款。特别在协议中明确第三方对数据的合法责任，确保在出现问题时，可以追溯责任；

2、审核数据来源：在接收第三方数据前，应进行数据来源审核，了解数据的收集、处理和存储过程，评估数据的真实性、准确性和完整性，确保数据来源合法；

3、审查数据内容：检查数据内容是否涉及违法违规信息，是否侵犯他人知识产权、涉嫌不正当竞争、违反公序良俗等。对于涉及个人信息、重要数据的，需要严格审查数据内容的合法性；

4、加强数据保护措施：可采用技术手段，如数据加密、数字签名等，确保数据在传输和存储过程中的安全性。

（六）通过软件程序或硬件设备等自动采集个人信息的合规要求

通过软件程序或硬件设备等方式（包括 SDK、API、浏览器、智能终端、传感器、摄像头等），在用户不知情或未经用户同意的情况下，采集和存储用户的个人信息，会导致用户隐私泄露、数据滥用等风险。为保护用户的合法权益，企业在采集、存储个人信息时需遵循合法原则，并做到以下要求：

1、App 通过申请获取移动智能终端提供的系统权限自动采集个人信息，应当说明自动采集个人信息的方式、时机、频次；

2、智能设备、应用软件的业务功能涉及后台运行时、长期监听时（如语音识别助手）自动采集个人信息的，还需说明安全措施、关闭方式等处理规则；

3、采集的个人信息涉及敏感个人信息的，说明处理敏感个人信息的必要性以及对个人权益的影响，还应当通过明确标识或突出显示等方式标注处理敏感个人信息相关的告知内容，以提醒个人予以重点关注；

4、涉及嵌入的第三方代码、插件（如 SDK 等）采集个人信息的，应说明第三方身份、采集个人信息的种类、目的、方式等；第三方代码、插件的提供方需向个人信息处理者主动披露采集个人信息的具体种类及处理规则，以免告知内容出现偏差。

第二十条　数据存储

（一）数据存储

企业应采取必要技术手段保障数据存储安全，防止数据泄露、损毁或被非法获取和恶意攻击，并做到如下要求：

1、数据加密：对存储的数据进行加密，确保数据在存储过程中不被未经授权或超越授权的第三方窃取；

2、数据脱敏：对敏感数据进行脱敏处理，降低数据泄露的风险；

3、数字签名：确保数据的完整性和真实性，防止数据在传输过程中被篡改；

4、数据泄露的防护：通过网络流量分析、应用接口探测、业务锚点检测等方法，及时发现并防止数据泄露事件；

5、云数据保护：针对云计算环境下的数据存储，采取相应的保护措施。

（二）数据备份

1、企业应根据数据的重要性、访问频率、价值和存储成本等因素，选择采用多种备份，如本地备份、异地备份、云备份等，以确保在某一备份系统中出现问题时，仍有其他备份系统可以恢复数据，并对备份数据进行加密，防止备份过程中的数据泄露；

2、企业应根据数据的重要性、访问频率、价值和存储成本等因素，选择计算机、固态硬盘、机械盘等合适的存储设备进行备份；

3、对数据实施全量备份、增量备份、差异备份等策略时，均制定相应的数据恢复预案，同时定期对备份数据进行恢复测试，确保备份数据的完整性和可用性。

（三）数据恢复

1、制定数据恢复预案：针对可能出现的数据丢失情况，能够快速、有效地进行恢复；

2、数据恢复管理权限：对数据恢复操作进行权限管理，确保只有经过授权的人员才能进行数据恢复；

3、数据恢复操作规范：在数据恢复过程中，遵循操作规范，避免因操作失误导致数据进一步丢失；

4、及时响应和处理：在发现数据丢失问题时，及时响应和处理，降低数据丢失带来的影响。

第二十一条　数据传输

为满足数据传输的合规要求，企业应做到如下要求：

1、企业可以采用对称加密、非对称加密和哈希算法等加密技术对数据进行加密，以防止数据在传输过程中被窃取或篡改，确保数据在传输过程中始终保持安全性；

2、数据传输方应充分告知数据接收方传输过程中的相关信息，包括数据来源、传输方式、存储时间等；

3、制定相应的数据传输管理制度，明确数据传输的责任人和操作流程，定期对数据传输系统进行安全审计，发现潜在的安全漏洞并及时修复；

4、选择安全可靠的传输介质，如光纤、专用通信线路等，并对数据传输过程中的访问权限进行严格控制，仅允许授权人员访问数据，降低内部数据泄露的风险；

5、制定数据传输安全应急预案，并在必要时进行实战演练，提高企业应对数据传输安全事件的能力。应急预案应包括数据泄露的应急处理流程、责任人及具体措施等。

第二十二条　数据交易

数据交易主体在数据交易过程中，应确保数据交易安全、合规和有序进行，数据交易合规的内容包括：

（一）一般要求

1、数据来源审核：数据交易前，数据提供方须确保数据来源合法并取得数据主体同意，遵循数据收集、处理、存储等方面的相关规定。法律、法规及相关政策明确规定开展数据采集应当取得特殊资质、许可、认证或备案的，数据提供方应当确认数据来源方已取得特殊资质、许可、认证或备案。

数据购买方在接收数据时，应核实并保留数据提供方的授权与许可文件；

2、数据内容审核：数据提供方提供的数据内容，须符合下列条件：

（1）征得数据主体同意和授权；

（2）不侵犯他人知识产权或商业秘密；

（3）不得损害其他经营者的合法权益，扰乱市场公平竞争秩序；

（4）不得有法律、法规规定禁止收集的其他数据。

3、数据交易合同签订：数据交易双方需签订书面合同，明确数据具有合法性、可控性、流通性及权属、用途、责任等方面的内容；

4、数据质量保障：数据交易中，数据提供方应确保数据的准确性、完整性、及时性、可靠性等。数据提供方还需建立健全数据质量检测、评估、审核和更新机制，防止侵犯知识产权、商业秘密等不良行为的发生，确保数据在交易过程中的质量稳定；

5、数据安全与保密：数据交易过程中，数据提供方和购买方需签订安全保密协议，明确双方在数据交易过程中的保密义务与责任。同时，采取技术手段保障数据传输、存储、使用等方面的安全，防止数据泄露、篡改等风险。

（二）重要数据交易合规

涉及国家安全、公共利益、民生保障等方面的重要数据交易的，通过订立书面协议，明确交易双方的数据安全责任，具体要求如下：

1、事前审批：涉及重要数据交易的，需按照法律、法规规定，履行事前审批程序；

2、数据保护：对重要数据进行加密、匿名化、脱敏等处理，确保数据交易过程中不存在泄露国家秘密、商业秘密和个人隐私的风险；

3、风险评估：在重要数据交易前，进行风险评估，识别潜在风险，制定相应措施；

4、紧急应对：建立突发事件应急处置机制和预案，对突发情况根据事件的性质、类型和影响及时进行处置。

第二十三条　数据使用

企业在使用数据过程中，应防止数据泄露、篡改、用户投诉等突发情况，并制定相应的应急措施进行预防，具体要求如下：

1、建立内部数据使用审查机制：对企业内部的数据使用进行规范和监督，对数据访问行为进行记录，以便在发生数据泄露时追查责任；

2、定期培训员工：定期对员工进行数据合规培训，树立数据合规意识，让员工了解并遵守最新的数据使用法规；

3、建立投诉处理机制：对数据使用过程中出现的用户投诉进行及时有效的处理；

4、数据安全事件应急响应机制：明确数据安全事件的应急响应流程、评估流程和证据固定流程，确保在发生数据泄露时能够迅速、有效地应对。

第二十四条　数据删除、销毁

企业应根据自身实际情况，制定合适的数据删除与销毁制度，确保数据的安全处理。

（一）数据删除的合规要求

1、全面覆盖：数据删除应确保涉及所有存储介质，包括内部服务器、硬盘、云存储、数据库、外部存储设备等；

2、不可恢复：数据删除应采用可靠的技术手段，确保删除后的数据无法恢复；

3、及时性：根据数据的重要性和敏感程度，设定合理的删除时间表，及时删除数据，使已不再需要的数据不会被未经授权或超越授权的人员获取，防止数据泄露事件的发生；

4、授权与审批：明确数据删除的审批及操作应获得相关授权，确保只有经过授权且在授权范围内的人员才能进行相关操作，并留存审批记录，以备查询；

5、记录与监控：对数据删除的具体步骤进行记录和监控，包括预处理、删除、验证等环节，确保删除操作合规；

6、应急预案：针对可能出现的问题和风险，制定应急预案，确保能够迅速、有效应对。

（二）数据销毁的合规要求

1、销毁方法：根据数据的敏感程度和存储介质，选择恰当的数据销毁方法，如物理销毁、擦写、消磁等；

2、验证销毁效果：对销毁过程进行验证，确保数据无法恢复；

3、存储介质安全：在销毁过程中，确保存储介质的物理安全、网络环境安全，防止数据泄露、窃取；

4、人员管理：对参与数据销毁的人员进行培训和监管，遵守合规要求；

5、应急预案：针对数据销毁过程中可能出现的问题，制定应急预案，确保销毁活动顺利进行。

第五章 数据出境

第二十五条 数据出境的合规要求

企业因业务需要向境外提供数据的，应当遵守《个人信息保护法》、《数据出境安全评估办法》、《个人信息出境标准合同办法》、《促进和规范数据跨境流动规定》等有关法律、法规的规定，全面梳理和处理出境的数据，对于按规定应申报数据出境安全评估、订立个人信息出境标准合同并备案、通过个人信息保护认证的，按照规定执行；提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使《个人信息保护法》规定权利的方式和程序等事项，并取得个人的单独同意。

第二十六条 数据出境的认定

符合下列情形之一的，属于数据出境：

（一）企业将在境内运营中收集和产生的数据传输至境外；

（二）企业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；

（三）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。

前款所称的境外，包括香港特别行政区、澳门特别行政区、台湾地区。

第二十七条　数据出境安全评估申报的适用范围

企业向境外提供数据，符合下列情形之一的，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：

（一）企业向境外提供重要数据；

（二）企业作为关键信息基础设施运营者向境外提供个人信息；

（三）企业作为非关键信息基础设施运营者自当年 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。

第二十八条　数据出境风险自评估

企业在申报数据出境安全评估前，应当开展数据出境风险自评估并形成书面自评估报告，自评估报告应包括下列内容：

（一）自评估工作情况。包括起止时间、组织情况、实施过程、实施方式等内容；

（二）出境活动整体情况。包括数据处理者基本情况、数据处理者安全保障能力情况、境外接收方情况、法律文件约定情况等，并详细说明拟出境数据情况；

（三）出境活动的风险自评估情况。按照《数据出境安全评估办法》第五条规定事项，说明数据出境风险自评估情况，重点说明自评估发现的问题和整改情况；

（四）自评估结论。综合风险自评估情况和相应整改情况，对拟申报的数据出境活动作出客观的风险自评估结论，充分说明得出自评估结论的理由。

第二十九条　个人信息出境标准合同备案和个人信息保护认证的适用范围

企业向境外提供个人信息，符合下列情形之一的，应当依法按照国家网信部门制定的标准合同与境外接收方订立个人信息出境标准合同，并向所在地省级网信部门备案或通过个人信息保护认证：

（一）企业作为非关键信息基础设施运营者，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）的；

（二）企业作为非关键信息基础设施运营者，自当年 1 月 1 日起，累计向境外提供不满 1 万人敏感个人信息的；

企业不得采取数量拆分等手段，将依法应当申报数据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。

第三十条　个人信息保护影响评估

企业向境外提供个人信息并向所在地省级网信部门备案前，应当开展个人信息保护影响评估并形成书面报告，评估报告应包括下列内容：

（一）个人信息提供者基本情况。包括：1.基本情况简介（股权结构、实际控制人、境内外投资情况、组织架构和个人信息保护机构信息等）；2.整体业务与处理个人信息情况；3.拟出境个人信息情况；

（二）境外接收方情况。包括：1.境外接收方基本情况；2.境外接收方处理个人信息的用途、方式等；3.境外接收方履行责任义务的管理和技术措施、能力等；

（三）个人信息提供者认为需要说明的其他情况；

（四）拟出境活动的影响评估情况。按照《个人信息出境标准合同办法》第五条规定事项，说明个人信息保护影响评估情况，重点说明评估发现的问题和整改情况；

（五）评估结论。综合影响评估情况和相应整改情况，对个人信息出境活动作出客观的影响评估结论，充分说明得出评估结论的理由和论据。

第三十一条　个人信息出境标准合同内容

个人信息出境标准合同，一般包括下列条款：

（一）个人信息处理者、境外接收方的名称、地址、联系方式、联系人等；

（二）个人信息处理者、境外接收方所负的合同义务；

（三） 境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响；

（四）个人信息主体的权利；

（五）个人信息主体救济的方式和途径；

（六）违约责任；

（七）争议解决的方法。

第三十二条　个人信息保护认证的原则和要求

企业应当根据 GB/T35273《信息安全技术个人信息安全规范》、TC260-PG-20222A《个人信息跨境处理活动安全认证规范》的要求，通过国家网信部门规定的专业认证机构的技术验证和现场审核后获发认证证书。

在认证证书的有效期内，认证机构采取获证后监督的方式，对企业进行持续监督，并合理确定监督频次。另外，认证机构要采取适当的方式实施获证后监督，确保获得认证的企业持续符合认证要求。

第三十三条　申报、备案、认证的豁免

企业向境外提供数据，符合下列条件之一的，可免于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：

（一）因国际贸易、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中不包含个人信息或者重要数据的；

（二）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；

（三）自由贸易试验区内的企业向境外提供负面清单外的数据；

（四）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（不包括重要数据）的；

（五）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（不包括重要数据）的；

（六）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（不包括重要数据）的；

（七）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（不含敏感个人信息及重要数据）的；

（八）国家网信部门规定的其他豁免情形。

第六章　法律责任

第三十四条　民事责任

企业开展数据处理活动违反法律、法规和强制性标准的规定，侵害他人权益并造成损害的，被侵权者有权请求企业承担停止侵害、排除妨碍、恢复原状、赔偿损失、赔礼道歉等民事责任。

第三十五条　行政责任

企业开展数据处理活动违反法律、法规和强制性标准的规定，经他人投诉、举报或数据监管部门依法履行职责中发现的，根据数据监管部门的要求，企业需承担下列行政责任：

（一）进行整改、消除隐患；

（二）改正，给予警告；

（三）罚款、没收违法所得；

（四）暂停相关业务、停业整顿；

（五）吊销相关业务许可证或者吊销营业执照。

企业承担相应行政责任的，对其直接负责的主管人员和其他直接责任人员处以罚款，并可禁止其在一定期限内担任相关企业的董事、监事、高级管理人员。

第三十六条　刑事责任

企业开展数据处理活动违反法律、法规和强制性标准的规定，构成犯罪的，可能以下列罪名进行定罪量刑：非法侵入计算机信息系统罪、非法获取计算机信息系统数据、非法控制计算机信息系统罪、破坏计算机信息系统罪、破坏计算机信息系统罪、拒不履行信息网络安全管理义务罪、侵犯公民个人信息罪、侵犯商业秘密罪等。

符合单位犯罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员判处相应刑罚。

第三十七条　法律责任的减免

企业违法进行数据处理活动，法律对企业以及其直接负责的主管人员和其他直接责任人员需承担的民事责任、行政责任、刑事责任有免除责任或减轻责任的情形另有规定的，依照其规定。

第七章　附则

第三十八条　基本概念

本指引所称的概念含义如下：

（一）数据，是指任何以电子或者其他方式对信息的记录；

（二）数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开、删除等活动；

（三）重要数据，特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，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；

（四）个人信息，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，包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等；

（五）敏感个人信息，是指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；

（六）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；

（七）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；

（八）数据合规，是指企业内部管理及其外部经营管理行为符合个人信息保护、网络安全、数据安全等数据法律、法规、强制性标准的要求；

（九）数据全生命周期，是指数据从产生，经过数据收集、数据存储、数据使用、数据加工、数据传输、数据提供、数据公开、数据删除和销毁等各种生存形态的演变过程；

（十）本指引所称的“以上”包括本数；所称的“不满”,不包括本数。

第三十九条　指引的解释

本指引由苏州市吴中区司法局、江苏万拓律师事务所负责解释。

第四十条　施行日期

本指引自发布之日起施行。

附:

本操作指引的起草由苏州市吴中区司法局、苏州大数据交易所进行指导，具体由江苏万拓律师事务所负责编写，各执笔律师简介如下:

王炳玉律师:江苏万拓律师事务所主任；

擅长领域:

数据合规与隐私保护、家族财富管理与传承

人工智能机器人产业链、股权投融资等法律服务；

联系电话:18505126656（同微信）

韩磊律师:江苏万拓律师事务所律师；

擅长领域:

民商事争议解决、公司治理、个人信息保护及数据合规;

华奕律师：江苏万拓律师事务所律师;

擅长领域:

民商事争议解决、公司法律事务、数据合规。

袁慧律师：江苏万拓律师事务所律师;

擅长领域:

公司治理、股权投融资、数据合规。

本操作指引最后由王炳玉律师负责统改定稿。

Chapter I General Provisions

Article 1 Purpose

The purpose of these guidelines is to guide enterprises in strengthening data compliance management, regulating data processing activities, protecting personal information, ensuring the security of enterprise data, promoting the compliant utilization of enterprise data, and providing support for enterprise development.

Article 2 Legal Basis

These guidelines are formulated in accordance with the Data Security Law of the People's Republic of China, Personal Information Protection Law of the People's Republic of China, Network Security Law of the People's Republic of China, Data Regulations of Suzhou, and other relevant laws and regulations.

Article 3 Scope of Application

Enterprises of various types in Wuzhong District may refer to these guidelines for conducting data compliance management in data processing activities. These guidelines are not mandatory. Where laws, regulations, and relevant national or industry standards have specific provisions on data compliance, such provisions shall prevail.

Article 4 Basic Principles

Enterprises conducting data processing activities shall adhere to the principles of legality, legitimacy, necessity, and good faith. They shall not engage in data processing activities that endanger national security or public interests, nor shall they harm the legitimate rights and interests of natural persons, juridical persons, or unincorporated organizations.

Chapter II Data Compliance Management System

Article 5 General Requirements

Enterprises engaging in data processing activities shall, in accordance with the provisions of laws and regulations, establish a sound specialized institution and operational mechanism for data compliance within the enterprise. They shall clarify the responsibilities and authorities of each institution and employee, organize data compliance training, and cultivate a compliance culture within the enterprise to effectively prevent and control legal risks in data processing activities.

Article 6 Responsibilities of the Person Responsible for Data Compliance

The person in charge of data compliance management is generally held by the legal representative or primary person in charge of the enterprise and shall undertake the following responsibilities:

(1) In accordance with the actual situation and industry characteristics of the enterprise, formulate appropriate data compliance strategies, and clearly define the

objectives, scope, and implementation plans of data compliance;

(2) Establish a dedicated data compliance department responsible for managing enterprise data compliance affairs, guiding data processing activities;

(3) Promote collaboration and communication among various departments within the enterprise to facilitate the smooth implementation of data compliance management;

(4) Provide necessary resource support for enterprise data compliance, including manpower, material resources, financial resources, etc., to ensure the effective operation of the compliance management system;

(5) Clarify the division of responsibilities among compliance management departments and personnel, and ensure that each department and individual possess the capabilities and authorities required for their duties. Simultaneously establish corresponding accountability mechanisms to drive effective implementation of data compliance policies;

(6) Establish a reporting and punishment mechanism for data violations;

(7) Receive reports on data compliance management, and provide guidance, supervision, and evaluation of it;

(8) Promote the formation of data compliance habits and atmosphere within the enterprise, transform employees' compliance concepts into compliant behaviors, and cultivate an enterprise data compliance culture.

Article 7 Responsibilities of the Data Compliance Department

Eligible enterprises shall establish a dedicated data compliance department. For enterprises where it is not necessary to establish a dedicated department, they may appropriately appoint data compliance officers who, together with the company's legal department, shall oversee data compliance management. They shall undertake the

following responsibilities:

(1) Based on the business needs of the enterprise and the requirements of laws, regulations, and mandatory standards, formulate systems, policies, and annual work plans for data compliance management, and promote their implementation;

(2) Regularly conduct compliance reviews of enterprise data processing activities, assess the legal risks involved, and ensure the compliance of business operations;

(3) Foster cross-departmental collaboration and communication to promote the implementation of data compliance work in various business areas;

(4) Organize data compliance training and promotional activities, and handle compliance inquiries from business departments and functional departments. Raise employees' awareness of data compliance to ensure that they adhere to data compliance requirements in their business operations;

(5) Regularly report the status of data compliance work to the person in charge of data compliance, propose improvement measures for compliance risks and issues, and provide decision-making support for enterprise data compliance management;

(6) Closely monitor the dynamics of national laws, regulations, industry policies, and standards, promptly adjust and enhance the enterprise's data compliance management system, ensuring that it meets the latest compliance requirements;

(7) Establish a sound data security emergency mechanism to respond to data security incidents and safeguard the legitimate rights and interests of the enterprise;

(8) Handle complaints and reports of data processing violations, provide opinions on classified disposal, and organize or participate in investigations of the violations;

(9) Assist in completing other data compliance-related tasks assigned by the person in charge of data compliance.

Article 8 Responsibilities of the Data Compliance Functional and Business Departments

The functional and business departments of the enterprise are at the forefront of data processing activities, responsible for the data compliance work within their respective departmental business scope, and undertake the following responsibilities:

(1) In accordance with the compliance regulations and policies established by the data compliance department, specify the implementation details of data compliance work within the department to ensure that departmental business activities comply with data compliance requirements;

(2) Participate in the formulation of compliance regulations and policies, provide business requirements and practical application scenarios, and enhance the feasibility and applicability of data compliance regulations and policies;

(3) Enhance data security protection measures, including encryption, access control, firewalls, and other technical measures, to ensure the security of data;

(4) Maintain close collaboration with other departments to jointly promote the smooth implementation of enterprise data compliance work;

(5) In the event of a data security incident, respond promptly, report to the data compliance department and the person in charge of data compliance, and cooperate in emergency response.

Article 9 Person in Charge of Personal Information Protection

Enterprises that process personal information to the amount specified by the national cyberspace administration shall designate a person in charge of personal information protection to supervise the activities related to the processing of personal

information and the implementation of protective measures.

The person in charge of personal information protection shall undertake the following responsibilities:

(1) Formulate relevant policies and measures for personal information protection in accordance with the laws, regulations, and the enterprise's compliance system, ensuring that the enterprise complies with regulatory requirements when handling personal information, and supervise the effective implementation of relevant policies and measures;

(2) Organize regular training and promotional activities related to personal information protection to enhance employees' awareness of and attention to personal information;

(3) Responsible for receiving and handling complaints and reports related to personal information protection, and promptly taking measures to address any existing issues;

(4) Regularly conduct personal information security impact assessments on enterprise personal information processing activities and initiate corrective actions based on the assessment results;

(5) In the event of an emergency involving personal information, immediate measures need to be taken to safeguard the security of personal information and report to the relevant regulatory authorities as required. Enterprises shall publicly disclose the contact information of the person in charge of personal information protection and submit the name, contact information, and other relevant details of the person in charge of personal information protection to the department that performs the duty of personal information protection.

Article 10 Data Compliance Obligations of Employees

To ensure that enterprise employees adhere to data compliance requirements in business operations, the enterprise shall implement the following requirements:

(1) During the recruitment, adherence to data compliance requirements and fulfillment of data compliance obligations shall be stipulated as conditions of employment;

(2) Specify the data compliance obligations of employees within the data compliance management system, including but not limited to data collection, storage, processing, and transmission processes;

(3) Necessary background checks shall be conducted on employees in key positions such as data analysis, system development, and security, to understand their civil litigation involvement, administrative penalties, criminal records, integrity, and credit status, ensuring that employees in key positions possess high moral qualities and compliance awareness;

(4) The enterprise shall specify the data compliance requirements and obligations that employees must adhere to through the signing of compliance commitments, confidentiality agreements, etc.;

(5) After employees holding key positions such as data analysis, system development, and security leave their positions or resign, the enterprise shall implement measures such as departure handover, audit, and declassification to ensure that they cannot access enterprise data.

Article 11 Reward Mechanism for Data Compliance

In data compliance management, enterprises shall implement reasonable incentive

measures for employees, which helps to enhance the initiative and awareness of employees in participating in data compliance work. Enterprises shall incorporate employees' performance in data compliance into assessment criteria such as material rewards, internal commendations, and promotion opportunities.

Article 12 Complaint, Reporting, and Rectification Mechanism

Enterprises shall establish a dedicated channel for reporting and complaints to promptly identify and rectify any data compliance violations. Additionally, the identity and information of whistleblowers and complainants must be kept confidential. Upon receiving complaints or reports, the enterprise's data compliance department shall promptly initiate an investigation. The investigation team shall possess professional knowledge and skills in data compliance to accurately assess whether the reported issues involve data violations. If data violations are indeed identified, the enterprise shall take appropriate corrective measures and provide feedback and public disclosure on the results of the investigation and rectification.

Chapter III Data Compliance Management Regime

Article 13 Data Classification and Grading System

Enterprises shall prioritize the management and protection of their data assets, conducting comprehensive sorting of their data assets and implementing classification and grading of data. The following requirements shall be met:

(1) Establish Objectives for Data Classification and Grading: Enterprises shall clearly define the objectives of data classification and grading to ensure that the

formulated system meets the actual needs of the enterprise;

(2) Develop Data Classification Standards: Enterprises shall develop unified data classification standards based on factors such as the business attribute and sensitivity of the data. These standards shall be scalable to accommodate changes in business operations.

(3) Set Data Grading Criteria: Enterprises shall establish reasonable data grading criteria based on factors such as the importance, sensitivity, and potential impact of data breaches. Further categorization shall include divided levels such as core data, important data, and general data to meet the security requirements of different data types.

(4) Implement Data Classification and Grading: Enterprises shall apply the formulated data classification and grading criteria to actual data management processes. It is essential for the enterprise to ensure that employees adhere to corresponding operational protocols such as access control, data encryption, and access log recording when accessing and handling data of different categories and levels.

(5) Optimize Data Classification and Grading System: Enterprises shall regularly review and optimize the data classification and grading system to adapt to the evolving needs of the enterprise and market changes.

Article 14 Risk Assessment Mechanism

Enterprises shall establish a data compliance risk assessment mechanism, and carry out data compliance risk assessment at least once a year. This assessment shall comprehensively review aspects such as the data compliance system, data processing procedures, data security measures, data alert and response mechanisms, etc. During the assessment process, potential risk points, compliance vulnerabilities, and security

breaches shall be analyzed, with a focus on identifying compliance risks that may arise from data processing activities, such as data leakage, improper collection, unreasonable usage, and potential consequences. A written assessment report shall be generated based on these findings. Based on the results of the risk assessment, the enterprise shall formulate corresponding risk response strategies. Assessment reports involving important data and core data shall be submitted to relevant supervisory authorities and regulatory departments.

Article 15 Safety Technical Protection Measures

After completing data classification and establishing a data resource directory, enterprises shall build corresponding technical protection systems tailored to different types and levels of data. This involves implementing data protection measures aligned with the types and levels of data, such as data backup, encryption, access control, firewall establishment, intrusion testing, and defense systems. Furthermore, security defenses shall be enhanced for data storage environments, data transmission processes, data access interfaces, and other network environments, ensuring that security technology protection is integrated throughout the data full life cycle.

Systems that process important data shall satisfy the requirements for level 3 or above network security protection and critical information infrastructure security protection, and systems that process core data shall be strictly protected in accordance with relevant regulations.

Article 16 Security Emergency Response Mechanism

Enterprises shall develop data security emergency plans, including specifying responsibilities, classifying security incidents, response procedures, etc., to address data security risks:

(1) Establish Data Security Emergency Management System: Clearly define the organizational structure, personnel responsibilities, and communication mechanisms to ensure that relevant departments can respond quickly and collaborate effectively when data security incidents occur;

(2) Classify Data Security Incidents: Classify data security incidents into different levels according to the degree of harm, scope of impact, and other factors, and formulate corresponding emergency response measures for each level;

(3) Data Security Incident Response Process: When facing security threats, enterprises shall take a series of orderly and efficient response measures to promptly detect, report, and respond to data security incidents:

1. Detect Security Incidents: Utilize monitoring devices, security auditing tools, etc., to conduct real-time monitoring of systems and networks, promptly identifying potential security risks.

2. Report Security Incidents: Upon discovering a security incident, promptly notify relevant responsible personnel, departments, or employees to ensure that they are aware of the security situation.

3. Analyze Security Incidents: Conduct in-depth analyses of security incidents to understand the causes, scope of impact, potential losses, etc., and clearly define the corresponding security incident levels.

4. Implement Emergency Response Measures: Implement the prepared response strategies based on the security incident level, including repairing and restoring

damaged systems and data.

5. Evaluate Response Effectiveness: After implementing response measures, assess the impact of the security incident and check the effectiveness of the response measures.

6. Regular Drills and Improvement: Organize regular security incident emergency drills to test the execution of incident discovery, notification, and response processes, continually optimizing data security incident handling measures, and enhancing actual response capabilities.

Article 17 Data Security Review Declaration Mechanism

Enterprises shall establish corresponding review standards and declaration mechanisms based on factors such as the scale of data and the involved fields. They shall actively conduct reviews to determine whether data processing activities may involve national security, economic operations, social stability, public health, and safety. Where conditions stipulated by laws and regulations are met, data security reviews shall be reported in accordance with relevant regulations.

The formulation of the enterprise's data security review declaration mechanism shall elaborate on review standards and procedures, specifying the scope, subjects, procedures, and time limits of the review. Additionally, the review standards shall possess a certain degree of flexibility to address the evolving landscape of data security.

Article 18 Data Compliance Training System

Enterprises shall organize training for employees in various departments to learn

about data protection laws, regulations, and standards, as well as specific requirements and methods of data compliance management. The purpose is to enhance employees' awareness and capabilities in data compliance, safeguard enterprise data security, and effectively mitigate legal risks inherent in data processing activities.

Chapter IV Compliance of the Data Full Life Cycle

Article 19 Data Collection

(1) Compliance Requirements for the Acquisition of Public Data by Automated Tools

Where enterprises use automated tools such as web crawlers to collect data, they shall ensure that the collection is legal and legitimate, comply with laws, regulations, industry self-discipline conventions, and the protocols and rules of the target website, and shall assess the performance of network services and the possible impacts, avoiding the interference with the normal functions of network services and the normal operation of computer information systems.

Enterprises that use automated tools to collect public data shall comply with the following requirements:

1. Enterprises shall not obtain data for unfair competition;

2. Enterprises shall not invade classified network and computer information systems to obtain data in violation of the law;

3. Enterprises shall not obtain data without authorization or beyond the scope of authorization by illegal acquisition of internal access, operating privileges, etc.;

4. Enterprises shall not interfere with the normal operation of the visited website or the normal operation of the computer information systems;

5. Enterprises shall not break through technical protections set up by the visited websites and computer information systems to protect data through technical decryption;

6. Where other circumstances prescribed by laws and regulations arise.

(2) Compliance Requirements for the Acquisition of Data by Purchase

Where enterprises acquire data through purchase, they shall conduct the necessary reviews on the qualifications of the data providers and the compliance of acquiring and holding the data. Purchasing data shall require the data providers to make lawful commitments on the sources, types, scope, and security of the data, and provide necessary verification. For data acquired through purchasing, enterprises shall assume equivalent responsibilities for security protection responsibilities and compliance obligations as for the data collected directly.

(3) Compliance Requirements for the Acquisition of Data by Exchange or Sharing

1. Before engaging in data exchange and sharing, enterprises shall specify the purpose, scope, and subjects involved in the data exchange; establish the background and motivations for the data exchange; clarify the recipients, types, and scale of shared data; and define the business areas and departments involved in the data exchange;

2. Enterprises shall execute a written agreement for data exchange and sharing. The agreement shall include requirements concerning data types, purposes of data usage, data storage periods, data security measures, data privacy protection, data compliance reviews, etc.;

3. During the process of data exchange and sharing, enterprises shall implement comprehensive measures for data security, including encryption, data masking, de-identification, and access controls, to ensure the security of data;

4. For data exchange and sharing activities, enterprises shall establish a regular review mechanism to conduct comprehensive and continuous supervision, enabling issues detected and rectified promptly. Additionally, enterprises shall enhance the management of sensitive and special data involved in the process of data exchange and sharing activities.

(4) Compliance Requirements for the Acquisition of Data during the Provision of Products and Services

1. Prior to the commencement of essential business of products or services (such as initial installation for individuals, first-time usage, or account registration), enterprises shall actively inform individuals of critical rules through evident notification (such as setting special user interfaces or separate steps) when displaying processing rules such as privacy policies via links. The notification shall include the chapter structures of the privacy policies (with clickable links for direct access to relevant chapters), types of personal information required for essential businesses, methods of data collection and purposes, as well as contact information for handling inquiries and complaints of personal data subjects. When collecting personal information, enterprises shall follow the principle of minimum necessity and only collect personal information directly related to the realization of the business function of products or services;

2. The privacy policy shall be drafted as a standalone document, separate from user agreements, user instructions, or any other documents. The privacy policy shall be easily accessible within four clicks from the main interface of the app, with a prominent and unobstructed link. The content of the privacy policy shall be presented in a readable format (including font size, font color, line spacing, etc.), avoiding small font size, dense text layout, faint text colors, or blurred text. The content of the privacy policy

shall be easy to understand, avoiding the use of obscure, verbose language that may be difficult for users to comprehend, such as the use of massive complex terms;

3. When developing new business functions and improving service experience, enterprises that collect personal information beyond the necessary scope shall obtain the consent of individuals. The provision of essential functions or services shall not be denied as individuals disagree with the provision of non-essential personal information;

4. Enterprises that use the data collected shall obtain the prior authorization and consent of the relevant data subject, ensuring that such consent does not exceed the scope of the information provided to the relevant data subjects;

5. When a product or service provides multiple business functions that require the collection of personal information, enterprises shall not force individuals to make batch consents on personal information or multiple data processing activities by bundling multiple business functions. An individual's refusal to consent should not affect the normal use of business functions unrelated to personal information.

(5) Compliance Requirements for Accepting the Third-Party Commission to Process Personal Information

Enterprises that accept the third-party commission to process personal information shall notify the individual of the recipient's name, contact information, processing purpose, processing method, and types of personal information, and obtain the individual's separate consent in accordance with the laws and the regulations.

Enterprises that accept the third-party commission to process personal information shall comply with the following requirements:

1. Execute a Data Processing Agreement: Prior to receiving third-party data, both parties shall enter into a written agreement outlining relevant matters such as the data source, purpose, confidentiality requirements, rights, and obligations. The agreement

shall include compliance commitments and provisions on breach liabilities. Specifically, the agreement shall stipulate the third party's legal liability concerning the data to ensure accountability in case of issues;

2. Examination of Data Source: Prior to the receipt of third-party data, enterprises shall undertake a thorough examination of the data source to comprehend the procedures of data collection, processing, and storage, while evaluating the authenticity, accuracy, and integrity of the data and ensuring the legality of the data source;

3. Examination of Data Content: Verify whether the data content includes any illegal or non-compliant information, infringes upon the intellectual property rights of others, engages in unfair competition, or violates public order and morals. For data involving personal information or critical information, a rigorous examination of the legality of the data content is required;

4. Enhance Data Protection Measures: Enterprises can employ technical measures such as data encryption, digital signatures, etc., to ensure the security of data during transmission and storage.

(6) Compliance Requirements for Automated Collection of Personal Information through Software Programs or Hardware Devices

The collection and storage of users' personal information through software programs or hardware devices (including SDK, API, browser, intelligent terminal, sensor, camera, etc.) pose risks of privacy breaches and data misuse when users are unaware or have not explicitly consented. To protect the legitimate rights of users, enterprises shall adhere to legal principles when collecting and storing personal information, and meet the following requirements:

1. When an application requests and obtains system permissions from intelligent terminals to collect personal information automatically, it shall specify the methods,

timing, and frequency of such automatic information collection;

2. For intelligent devices and application software that involve the automatic collection of personal information in the backend or continuous monitoring (such as speech recognition assistants), it is also necessary to specify the processing rules such as security measures and shutdown methods;

3. If the collected personal information includes sensitive personal information, it is necessary to explain the necessity of processing such sensitive personal information and the impact on individual rights. Additionally, the notification content concerning sensitive personal information shall be clearly identified or highlighted to remind individuals to pay close attention;

4. Where third-party codes or plugins (such as SDK) have the function of collecting personal information, enterprises shall specify the identity of the third party, the types of collected personal information, the purposes of collection, and the methods used. The provider of third-party code or plugins shall proactively inform the personal information processor of the specific types and the processing rules of collected personal information to avoid any deviation in the notification content.

Article 20 Data Storage

(1) Data Storage

Enterprises shall adopt necessary technical means to ensure the security of data storage, safeguarding data against breaches, destruction, unauthorized access, and malicious attacks, and shall comply with the following requirements:

1. Data Encryption: Encrypt stored data to ensure that data is not accessed by unauthorized or beyond authorized third parties during storage;

2. Data Masking: The process of masking sensitive data to reduce the risk of data

breaches;

3. Digital Signature: Ensures the integrity and authenticity of data, preventing data tampering during transmission;

4. Protection against Data Breaches: Utilizing methods such as network traffic analysis, API (Application Programming Interface) probe, and PGW (Packet Data Network Gateway) test to promptly detect and prevent data breaches;

5. Protection of Cloud Data: Enterprises that use cloud computing to conduct data storage shall take security protection measures.

(2) Data Backup

1. Enterprises shall select multiple backup methods, such as local backup, remote backup, and cloud backup, based on the importance, access frequency, value, and storage costs of the data. This ensures that when a problem occurs in a backup system, the data can still be recovered from other backup systems. Additionally, backup data should be encrypted to prevent data breaches during the backup;

2. Enterprises should select appropriate storage devices such as computers, solid-state drives (SSDs), and mechanical hard drives for backup based on the importance, access frequency, value, and storage costs of the data;

3. When performing full backups, incremental backups, differential backups, and other backup strategies, corresponding data recovery plans shall be established. Regular recovery tests of backup data shall be conducted to ensure the integrity and availability of the backup.

(3) Data Recovery

1. Establish Data Recovery Plans: Establish plans for data recovery to efficiently and promptly restore data in data loss scenarios;

2. Data Recovery Access Management: Implement access controls for data recovery to ensure that only authorized personnel are permitted to undertake data recovery tasks;

3. Standardized Procedures for Data Recovery: Adhere to standardized procedures during data recovery operations to prevent further data loss resulting from operational errors;

4. Prompt Response and Handling: Respond promptly and effectively upon discovering data loss issues to mitigate the impact of data loss.

Article 21 Data Transmission

Enterprises shall comply with the following requirements to be in accordance with compliance requirements for data transmission:

1. Enterprises may utilize encryption technologies such as symmetric encryption, asymmetric encryption, and Secure Hash Algorithm to encrypt data, thereby preventing data theft or data tampering during transmission, and ensuring data remains secure throughout the transmission;

2. The data transmitting party shall fully inform the data receiving party of the relevant information during the transmission process, including the data source, transmission method, and storage duration;

3. Enterprises shall establish data transmission management systems, define the responsible person and operational procedures for data transmission, conduct regular security audits on data transmission systems, identify potential security vulnerabilities, and promptly address and repair them;

4. Enterprises shall select secure and reliable transmission mediums, such as fiber optics and dedicated communication lines, and rigorously control access permissions

during data transmission. To minimize the risk of internal data breaches, only authorized personnel own access to the data;

5. Enterprises shall establish data transmission security contingency plans and conduct practical drills to enhance the ability to respond to incidents during data transmission. The contingency plan shall include the emergency response procedures for data breaches, the responsible person, and specific measures.

Article 22 Data Transaction

The participants involved in data transactions shall ensure that the transaction is conducted securely, compliantly, and in an orderly manner. The compliance requirements for data transactions include:

(1) General Requirements

1. Examination of Data Source: Prior to the data transaction, the data provider shall ensure the legality of data sources and obtain consent from data subjects, adhering to relevant regulations on data collection, processing, storage, etc. Where laws, regulations, and related policies explicitly require special qualifications, permits, certifications, or filings for data collection activities, the data provider shall ensure that the data source has obtained such special qualifications, permits, certifications, or filing.

The data purchaser shall verify and retain the data provider's authorization and licensing documents when receiving data;

2. Data Contents Review: The data content provided by the data provider must comply with the following conditions:

1) Enterprises shall obtain consent and authorization from the data subject;

2) Enterprises shall not infringe upon the intellectual property rights or trade secrets of others;

3) Enterprises shall not harm the legitimate rights and interests of other operators or disrupt the fair market competition order;

4) Enterprises shall not collect any other data prohibited by laws and regulations.

3. Signing of the Data Transaction Contract: Both parties involved in the data transaction shall enter into a written contract to specify the legality, controllability, transferability, ownership, purpose, responsibilities, and other relevant aspects of the data;

4. Data Quality Assurance: In the data transaction, the data provider shall ensure the accuracy, integrity, timeliness, and reliability of the data. The data provider shall also establish and improve a sound mechanism for data quality testing, assessment, auditing, and updating to prevent infringement of intellectual property rights, trade secrets, and other misconducts. This is to ensure the stability of data quality throughout the transaction;

5. Data Security and Confidentiality: During the data transaction, the data provider and the purchaser shall enter into a security and confidentiality agreement to clearly define the confidentiality obligations and responsibilities of both parties. Additionally, technical measures shall be implemented to ensure the security of data transmission, storage, and usage, preventing risks such as data breaches and tampering.

(2) Compliance Requirements for Transactions of Important Data

For transactions of important data involving national security, public interests, and livelihood security, both parties shall establish a written agreement to delineate their data security responsibilities. Specific requirements are as follows:

1. Prior Approval: Transactions involving important data shall fulfill the prior approval procedures as stipulated by laws and regulations;

2. Data Protection: Important data shall be subjected to encryption, anonymization,

masking, or de-identification to ensure that there is no risk of disclosing state secrets, business secrets, or personal privacy during the data transaction;

3. Risk Assessment: Prior to transactions of important data, a risk assessment shall be conducted to identify potential risks and formulate corresponding measures;

4. Emergency Response: Establish emergency response mechanisms and plans to deal with unforeseen incidents promptly according to the nature, type, and impact of the incidents.

Article 23 Data Usage

In the course of using data, enterprises shall prevent data breaches, data tampering, user complaints, and other emergencies, and establish emergency response measures for prevention. Specific requirements are as follows:

1. Establish a Review Mechanism for Internal Data Usage: Standardize and supervise internal data usage, and record data access activities to enable accountability tracing in case of data breaches;

2. Conduct Regular Employee Training: Conduct periodic data compliance training for employees to cultivate their awareness of data compliance, enabling employees to understand and adhere to the latest data usage regulations;

3. Establish Complaint Handling Mechanisms: Promptly and effectively address user complaints arising from data usage processes;

4. Emergency Response Mechanism for Data Security: Define the emergency response procedures, assessment process, and evidence preservation process for data security to ensure prompt and effective responses in the event of data breaches.

Article 24 Data Deletion and Destruction

Enterprises shall establish appropriate data deletion and destruction systems in light of their realities to ensure the secure processing of data.

(1) Compliance Requirements for Data Deletion

1. Comprehensive Coverage: Data deletion shall ensure the coverage of all storage media, including internal servers, hard drives, cloud storage, databases, external storage devices, etc.;

2. Irrecoverability: Data deletion shall employ reliable technical means to ensure that the deleted data can not be recovered;

3. Timeliness: Based on the importance and sensitivity of the data, set a reasonable deletion schedule to promptly delete data that is no longer needed. This prevents unauthorized obtaining of data from individuals unauthorized or beyond authorization, and prevents the risk of data breaches;

4. Authorization and Approval: It is required to obtain relevant authorization for the approval and operation of data deletion, ensuring that only authorized personnel within the authorization period can perform related operations. Approval records shall be retained for future reference;

5. Recording and Monitoring: Record and monitor the specific steps of data deletion, including pre-processing, deletion, verification, etc., to ensure that the deletion operation is compliant;

6. Emergency Response Plan: Make an emergency response plan for potential issues and risks to ensure prompt and effective response.

(2) Compliance Requirements for Data Destruction

1. Destruction Method: Select appropriate data destruction methods according to

the sensitivity and storage medium of the data, such as physical destruction, erasure, degaussing, etc.;

2. Verification of the Destruction Effect: Verify the destruction process to ensure that the data cannot be recovered;

3. Storage Media Security: During the destruction process, ensure the physical security and network environment security of the storage media, so as to prevent data leakage and theft;

4. Personnel Management: Train and supervise personnel involved in data destruction to ensure that they comply with compliance requirements;

5. Emergency Response Plan: Make an emergency response plan for potential issues that may arise during the data destruction process to ensure the smooth progress of destruction activities.

Chapter V Data Cross-Border Transfer

Article 25 Compliance Requirements for Data Exit

Enterprises that provide data to foreign countries for business purposes, shall comply with relevant laws and regulations such as the Personal Information Protection Law, Measures for Security Assessment of Data Export, Measures for Standard Contract of Cross-border Transfer of Personal Information, and Provisions on Promoting and Regulating Cross-border Data Flows. Enterprises shall comprehensively sort out and process the exported data. Those who are required to apply for the data exit security assessment, complete the record-filing of the personal information exit standard contract, or pass the certification for personal information protection, shall comply with the regulations. For those providing personal information, they shall

inform individuals of overseas recipients' designation or name, contact information, processing purpose, processing method, types of personal information, and the ways and procedures for individuals to exercise their rights under the Personal Information Protection Law to overseas recipients, and obtain individuals' separate consent.

Article 26 Identification of Data Exit

The following situations fall into data exit:

(1) Enterprises transfer the data collected and generated in domestic operations to overseas;

(2) Data collected and generated by enterprises are stored domestically, but can be inquired, retrieved, downloaded, or exported by overseas institutions, organizations, or individuals;

(3) Other data processing activities such as processing personal information of domestic natural persons overseas as specified in the second paragraph of Article 3 of the Personal Information Protection Law.

The term "overseas" in the preceding paragraph includes the Hong Kong Special Administrative Region, the Macao Special Administrative Region, and the Taiwan Region.

Article 27 Applicable Scope for Declaration of Data Exit Security Assessment

Enterprises that provide data to foreign countries meet one of the following conditions shall declare the outbound data transfer security assessment to the national

cyberspace administration through the local provincial cyberspace administration:

(1) Enterprises provide important data to foreign countries;

(2) As critical information infrastructure operators, enterprises provide personal information to foreign countries;

(3) As non-critical information infrastructure operators, enterprises have cumulatively provided personal information to overseas of more than 1,000,000 individuals (excluding sensitive personal information) or sensitive personal information to more than 10,000 individuals since January 1 of the current calendar year.

Article 28 Self-assessment of Data Exit Risks

Before applying for the data exit security assessment, enterprises shall carry out a self-assessment of data exit risks and form a written self-assessment report. The self-assessment report shall include the following contents:

(1) Details of the self-assessment work, including starting and ending time, organizational structure, implementation process, and methods used;

(2) Overview of the export activities, including the basic information about data processors, security capabilities of data processors, information about the overseas recipients, legal document agreements, etc., and a detailed description of the data intended for export;

(3) Risk self-assessment of the exit activities. In accordance with Article 5 of the Measures for Security Assessment of Data Export, the self-assessment of data exit risks shall be explained and the problems found in the self-assessment and rectification shall be emphasized;

(4) Conclusion of the self-assessment. Synthesize the risk self-assessment and corresponding rectification, make an objective risk self-assessment conclusion on the

data exit activities to be declared, and fully explain the reasons for the conclusion.

Article 29 Applicable Scope of Personal Information Exit Standard Contract Filing and Personal Information Protection Certification

Enterprises that provide personal information to foreign countries and meet one of the following conditions shall legally complete personal information exit standard contracts with overseas recipients in accordance with the standard contracts set by the national cyberspace administration, and file with the local provincial cyberspace administration or pass the certification for personal information protection:

(1) As non-critical information infrastructure operators, enterprises have cumulatively provided personal information (excluding sensitive personal information) to overseas of more than 100,000 individuals but less than 1000,000 individuals since January 1 of the current calendar year;

(2) As non-critical information infrastructure operators, enterprises have cumulatively provided sensitive personal information to overseas of less than 10,000 individuals since January 1 of the current calendar year;

Enterprises are prohibited from using methods such as quantity splitting to provide personal information that shall be declared for data exit security assessment in accordance with the law to overseas through the method of establishing standard contracts.

Article 30 Impact Assessment of Personal Information Protection

Before providing personal information to foreign countries and filing with the

local provincial cyberspace administration, enterprises shall conduct an impact assessment of personal information protection and form a written report. The assessment report shall include the following contents:

(1) Basic information of personal information providers, including 1) brief introduction to basic information (equity structure, actual controller, domestic and foreign investment situation, organizational structure, and information about personal information protection agencies, etc.); 2) overall business and personal information processing situation; 3). intended export personal information situation;

(2) Information on overseas recipients, including: 1) basic information, 2) purposes and methods of processing personal information, etc.; 3) management, technical measures, and capabilities for fulfilling responsibilities and obligations;

(3) Other circumstances that personal information providers deem necessary to explain;

(4) Impact assessment of intended export activities. According to Article 5 of the Measures for Standard Contract of Cross-border Transfer of Personal Information, the impact assessment of personal information protection shall be explained and the problems found in the assessment and rectification shall be emphasized;

(5) Conclusion of the assessment. Synthesize the impact assessment and corresponding rectification, make an objective impact assessment conclusion on the personal information exit activities, and fully explain the reasons and arguments for the conclusion of the assessment.

Article 31 Contents of Personal Information Exit Standard Contracts

A personal information exit standard contract generally includes the following clauses:

(1) Name, address, contact information, and contact person of the personal information processors and the overseas recipients;

(2) Contractual obligations of the personal information processors and the overseas recipients;

(3) Impact of the data protection policies and regulations of the country or region where the overseas recipients are located on the performance of the contract;

(4) Rights of personal information subjects;

(5) Remedies available to personal information subjects;

(6) Liability for breach of contract;

(7) Dispute resolution methods.

Article 32 Principles and Requirements for Personal Information Protection Certification

In accordance with the requirements of GB/T35273 Information Security Technology-Personal Information Security Specification and TC260-PG-20222A Security Certification Specification for Cross-border Processing Activities of Personal Information, enterprises shall obtain the certification certificate after passing the technical verification and on-site audits of the professional certification bodies stipulated by the national cyberspace administration.

During the validity period of the certification certificate, the certification bodies shall conduct continuous supervision of the enterprises after they obtain the certificate, and reasonably determine the frequency of supervision. Additionally, the certification bodies shall take appropriate measures to implement post-certification supervision to ensure that certified enterprises continue to meet the certification requirements.

Article 33 Exemptions from Declaration, Filing, and Certification

Enterprises that provide data to foreign countries and meet any of the following conditions are exempted from applying for the data exit security assessment, completing the personal information exit standard contracts, and passing the certification for personal information protection:

(1) Data collected and generated in international trade, cross-border transportation, academic cooperation, cross-border production and manufacturing, marketing, and other activities without personal information or important data;

(2) Personal information collected and generated overseas, transferred to the domestic for processing, and then provided to overseas without introducing domestic personal information or important data in the process;

(3) Enterprises in the pilot free trade zones provide data outside the negative list to overseas;

(4) It is really necessary to provide personal information to overseas (excluding important data) for the establishment and performance of contracts where individuals act as one of the parties, such as cross-border shopping, cross-border delivery, cross-border remittances, cross-border payments, cross-border account opening, flight and hotel reservations, visa processing, examination services, etc.;

(5) It is really necessary to provide employees' personal information (excluding important data) to overseas when implementing cross-border human resources management according to legally formulated labor rules and regulations and legally signed collective contracts;

(6) It is really necessary to provide personal information (excluding important data) to overseas in emergencies to protect the life, health, and property safety of natural persons;

(7) Data processors, other than critical information infrastructure operators cumulatively provide personal information (excluding sensitive personal information and important data) to overseas less than 100,000 individuals since January 1 of the current calendar year;

(8) Where other exemption circumstances prescribed by the national cyberspace administration.

Chapter VI Legal Liability

Article 34 Civil Liability

If enterprises conduct data processing activities that violate laws, regulations, and mandatory standards, which infringe upon the rights and interests of others and cause harm, the aggrieved party has the right to request the enterprises to bear civil liabilities such as cessation of infringement, removal of obstacles, restoration of the original state, compensation for losses, and apology.

Article 35 Administrative Liability

If enterprises conduct data processing activities that violate laws, regulations, and mandatory standards and are complained or reported by others, or discovered by the data regulatory authority in the performance of its duties, the enterprises must bear the following administrative responsibilities as required by the data regulatory authority:

(1) Enterprises shall conduct rectification and eliminate hidden dangers;

(2) Enterprises shall make corrections and receive warnings;

(3) Enterprises shall be subject to fines and confiscation of illegal gains;

(4) Enterprises shall suspend relevant business operations and temporarily close for rectification;

(5) Enterprises shall have their relevant business permits or business licenses revoked.

If enterprises bear corresponding administrative liabilities, fines will be imposed on the directly responsible managers and other directly responsible personnel, and they may be prohibited from serving as directors, supervisors, or senior management personnel of related companies for a certain period.

Article 36 Criminal Liability

If enterprises conduct data processing activities that violate laws, regulations, and mandatory standards, and constitute a crime, the following charges may be used for conviction and sentencing: crime of illegal intrusion into computer information systems, crime of illegal acquisition of computer information system data, crime of illegal control of computer information systems, crime of destroying computer information systems, crime of refusing to fulfill information network security management obligations, crime of infringing on citizens' personal information, crime of infringing on trade secrets, etc.

For unit crimes, fines shall be imposed on the entity, and corresponding penalties shall be imposed on its directly responsible managers and other directly responsible personnel.

Article 37 Reduction or Exemption of Legal Liability

If enterprises conduct illegal data processing activities and there are other provisions in the law that exempt or mitigate the civil, administrative, and criminal liabilities that the enterprises, as well as their directly responsible managers and other directly responsible personnel, shall be applied in accordance with their provisions.

Chapter VII Supplementary Provisions

Article 38 Basic Concepts

The conceptual meanings mentioned in these guidelines have the following meanings:

(1) Data refers to any record of information by electronic or other means;

(2) Data processing includes activities such as data collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.;

(3) Important data refers to data in specific fields, groups, regions, or data that reaches a certain level of accuracy and scale, once leaked, tampered with, or destroyed, may directly endanger national security, economic operation, social stability, public health, and safety;

(4) Personal information refers to various information related to identified or identifiable natural persons recorded in electronic or other forms, excluding anonymized information. It includes name, date of birth, ID card numbers, personal biometric information, addresses, communication and contact information, communication records and content, account password, property information, credit information, travel trajectory, accommodation information, health and physiological

information, transaction information, etc.;

(5) Sensitive personal information refers to personal information that, once leaked or illegally used, could easily lead to the infringement of natural person's personal dignity or the endangerment of their personal and property safety, including biometric identification, religious beliefs, specific identities, medical health, financial accounts, travel trajectories, and personal information of minors under the age of fourteen;

(6) Key information infrastructure refers to important network facilities and information systems, etc., in critical industries and fields such as public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, national defense technology industry, and other sectors that, once destroyed, lost in function, or data leaked, could seriously endanger national security, national economy, people's livelihood, and public interests;

(7) Data security refers to the ability to take the necessary measures to ensure the effective protection and legal use of data, as well as the ability to guarantee a continuous state of security;

(8) Data compliance refers to enterprises' internal management and external business management behaviors comply with the requirements of data laws, regulations, and mandatory standards such as personal information protection, network security, data security, etc.;

(9) Data full life cycle refers to the evolutionary process of data through various forms of survival, from generation to data collection, data storage, data usage, data processing, data transmission, data provision, data disclosure, data deletion, and destruction;

(10) The term "more than" in these guidelines includes the number, and "less than" does not include the number.

Article 39 Interpretation of These Guidelines

These guidelines shall be subject to interpretation by the Judicial Bureau of Wuzhong District, Suzhou City, and Vanto Law Firm.

Article 40 Date of Implementation

These guidelines shall come into force as from the date of promulgation.

Annex:

The drafting of these guidelines is guided by the Judicial Bureau of Wuzhong District, Suzhou City, and the Suzhou Big Data Exchange, with specific composition by Vanto Law Firm. Brief introductions of the drafting lawyers are as follows:

Wang Bingyu, Esq.: Director of Vanto Law Firm;

Areas of expertise:

Data compliance and privacy protection, family wealth management, and inheritance

Legal services for the artificial intelligence robot industry chain and equity investment and financing, etc.;

Contact number: 18505126656 (same as WeChat)

Han Lei, Esq.: Lawyer at Vanto Law Firm;

Areas of expertise:

Civil and commercial dispute resolution, corporate governance; personal information protection and data compliance;

Hua Yi, Esq.: Lawyer at Vanto Law Firm;

Areas of expertise:

Civil and commercial dispute resolution, corporate legal affairs, and data compliance.

Yuan Hui, Esq.: Lawyer at Vanto Law Firm;

Areas of expertise:

Corporate governance, equity investment and financing, and data compliance.

The final revision of these operation guidelines is undertaken by Lawyer Wang Bing Yu for overall editing and finalization.