上海数据交易所
数据交易安全合规指引

上海数据交易所
SHANGHAI DATA EXCHANGE

上海数据交易所
数据交易安全合规指引

目 录

一、总则

第一条【指引目的】

为进一步加强数据交易主体关于数据交易合规与安全的理解和认知，引导交易主体合规、安全开展数据交易，本所根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《上海市数据条例》等法律法规，结合本所数据交易实际，制定本指引。

第二条【基本要求】

开展数据交易时，数据交易主体应当遵守以下基本要求:

（一）遵守我国关于数据流通与交易管理的法律法规，尊重社会公德、商业道德，服从监督管理;

（二）采取必要措施，做到交易过程可控制、风险可防范、责任可追溯、合规性可监督;

（三）数据交易主体应当诚实守信，恪守承诺，全面及时履行合同约定及相关承诺;

（四）数据交易主体在享有数据权益的同时，应当履行相关义务，确保数据交易安全合规。

第三条【适用范围】

数据交易主体在本所进行数据交易与相关服务活动时，可参照指引规定开展数据交易。

二、主体合规要求

第四条【主体资质】

主体资质是进行有效数据交易的基础要件，为保障数据

交易安全，数据交易主体资质应当满足下列要求:

（一）系依法成立并有效存续的法人、非法人组织;

（二）具有良好的商业信誉，近一年内无重大数据类违法违规记录且未出现重大网络和数据安全事故;

（三）法定代表人、董事、监事不存在重大数据类违法违规行为、被列为失信被执行人以及其他可能对数据交易活动构成实质性重大不利影响的情形;

（四）不存在可能对数据交易活动构成实质性重大不利影响的其他情形。

第五条【合规经营能力】

合规经营能力是数据交易主体进行有效数据交易的重要要素，为保障数据交易安全，在本所开展数据交易的，应当满足下列持续合规经营能力要求:

（一）不存在影响持续经营的重大财务风险;

（二）不存在影响持续经营的担保、诉讼以及仲裁等重大事项;

（三）不存在影响持续经营能力的其他情形。

三、数据安全管理体系

第六条【数据安全管理制度】

为降低数据交易和流通风险，数据交易主体应当积极履行数据安全保护义务，建立健全全流程数据安全管理制度，采取相应的技术措施和其他必要措施，确保数据在安全的基础上有序流通。

第七条【数据安全管理部门】

设立数据安全管理部门，承担以下职责:

（一）在全面梳理业务和现有资源的基础上，充分评估各相关部门在日常处理数据活动中的主要风险，明确数据全生命周期的安全要求;

（二）结合业务需求、监管要求、自身能力，确定企业数据安全目标，制定数据安全战略;

（三）指定人员实施内部数据安全管理工作，明确工作职责与任务;

（四）制定与完善数据安全管理规范体系并推动其有效实施;

（五）统筹实施数据安全管理工作，监督落实数据安全管理制度及技术防护措施执行情况，对数据处理活动定期开展数据安全风险评估;

（六）建立安全风险监测体系，采取措施监控内部数据处理活动和外部访问活动，防范不正当的数据访问和处理行为;

（七）建立数据安全事件应急管理制度，制定数据安全事件应急预案并定期进行演练，及时处置数据安全风险和事件;

（八）定期对员工进行数据安全宣传教育培训并考察员工能力与岗位职责的匹配程度;

（九）建立数据安全投诉受理、调查与督导机制，督促企业落实数据安全保护义务。

第八条【数据分类分级保护及管理】

数据交易主体在对数据进行全面梳理时，可参照国家标准和行业标准，结合自身业务对数据进行分类分级，形成目录清单并采取相匹配的保护和管理措施。

第九条【数据全生命周期安全管理】

数据交易主体应当建立数据全生命周期安全管理制度，针对不同类型和级别数据，实施数据收集、存储、使用、加工、传输、提供、销毁等环节的保护与管理，保障数据的保密性、完整性、可用性和合规性。

第十条【数据安全技术保护体系】

数据交易主体应当结合数据应用场景以及数据分类分级情况，可建立覆盖数据全生命周期的安全防护机制，采取数据加密、数据脱敏、身份认证、入侵防护、安全监测等技术保护措施，提高数据安全保障能力。

第十一条【数据安全人员】

数据交易主体需明确关键岗位人员及员工数据安全问责规范，可通过制定可行的管理制度和操作规程、数据安全培训及考核等方式提升企业员工的数据安全意识。

第十二条【数据安全事件应急响应机制】

数据交易主体应当制定数据安全事件应急预案，积极开展数据安全应急演练，提高对数据安全事件的预防和应对能力。

四、数据来源合法

第十三条【收集公开数据的要求】

数据交易供方使用自动化工具收集公开数据的，应当符合以下要求:

（一）不得以不正当竞争为目的，违反诚实信用获取数据;

（二）不得违法侵入涉密网站和计算机信息系统获取数据;

（三）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;

（四）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;

（五）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;

（六）未征得相关主体同意的，不得收集涉及他人知识产权、商业秘密或者非公开的个人信息的数据;

（七）法律法规规定的其他要求。

第十四条【自行生产数据的要求】

数据交易供方在生产经营活动中产生的或通过自身信息系统生产的数据，应确保数据的生产和处理行为合法，不存在侵犯第三方合法权益的情形。

第十五条【协议获取数据的要求】

数据交易供方通过采购、共享、授权许可等方式获取数据的，应当符合以下要求:

（一）保存数据采购协议、共享或授权许可文件。前述协议或文件内容应当约定数据交易供方取得对相关数据的授权使用、加工、对外提供等相应权利;

（二）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，数据交易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;

（三）确认数据来源方向数据交易供方提供数据获取渠道合法、权利清晰无争议的承诺;

（四）法律法规及相关政策规定的其他要求。

第十六条【收集个人信息的要求】

数据交易供方在生产经营活动中收集个人数据的，需确保个人信息的收集具有明确、合理的目的，并遵循合法正当、最小必要、告知同意等原则。具体要求如下:

（一）基于个人同意处理个人信息的，仅收集与实现产品或服务的业务功能直接相关的个人信息，并且限于实现处理目的最短周期、最低频次，采取对个人权益影响最小的方式;

（二）数据交易供方应当按照法律法规要求获得个人信息主体的同意或单独同意，并能够提供相关证明材料;

（三）交易数据涉及个人信息处理的，应当事先进行个人信息保护影响评估或取得个人信息保护认证;

（四）采取去标识化、匿名化等安全技术措施，防止未经授权的访问以及个人信息泄露、篡改和丢失;

（五）法律法规规定的其他要求。

五、数据产品的可交易性

第十七条【可交易性定义】

数据产品的可交易性是指在数据来源合法的基础上，该类数据形成的数据产品具有合法性、可控性、流通性。为保障数据交易的合法合规，数据交易供方应当确认其提供的数据产品属于法律法规允许交易的范围，数据处理符合法律规定，不包含禁止交易的数据。

第十八条【数据产品内容合法合规】

数据产品不得含有危害国家安全、违反公序良俗或侵害他人合法权益的违法信息，具体要求如下:

（一）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的;

（二）损害国家荣誉和利益的;

（三）歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的;

（四）宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的;

（五）煽动民族仇恨、民族歧视，破坏民族团结的;

（六）破坏国家宗教政策，宣扬邪教和封建迷信的;

（七）散布谣言，扰乱经济秩序和社会秩序的;

（八）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的;

（九）侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的;

（十）以违反诚实信用的方式不正当获取和使用他人数据，严重损害其他经营者和消费者的合法权益，扰乱市场公平竞争秩序的;

（十一）其他法律法规禁止的内容。

第十九条【重要数据交易合规】

数据产品涉及重要数据的，应当符合相关法律法规规定后方可开展交易，具体要求如下:

（一）自行或者委托数据安全服务机构进行安全风险评估，评估结果不存在危害国家安全、公共利益的情形的;

（二）订立书面协议，明确交易双方的数据安全责任;

（三）对数据交易需方的安全保护能力、资质进行核验;

（四）法律法规规定需要征得相关部门同意的，应当取得同意。

第二十条【实质性加工和创新性劳动】

数据交易供方应当说明数据产品的知识投入情况和注入劳动情况。数据处理过程包括对原始数据进行必要的数据脱敏、清洗、标注、整合、分析，通过算法运用、深度融合等方法形成数据产品。

第二十一条【数据产品应用场景与使用条件】

法律法规对数据产品应用场景、使用对象等有特别规定的，数据交易双方应当从其规定。

第二十二条【数据产品出境合规】

数据交易供方向境外提供数据产品，需符合以下要求：

（一）需要申报数据出境安全评估的，应当按照国家网信部门要求，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，并履行数据安全保护责任和义务；

（二）无需向国家网信部门申报数据出境安全评估，但涉及个人信息出境的，应当遵照法律法规规定的数据出境要求开展数据出境活动，并履行法律法规及相关政策规定的其他义务。

第二十三条【数据交易协议内容合规】

数据交易双方应当签署数据交易协议，确保协议内容合法合规，不侵犯他人合法权益，并应当至少包含以下条款：交易数据的用途、使用范围、交付方式、使用期限、安全义务、交易价格、保密约定、争议解决等。

六、附则

第二十四条【修订与解释】

本指引由上海数据交易所负责修订与解释。

第二十五条【实施日期】

本指引自发布之日起实施。

附件：数据交易主体可参考的法律法规与标准

可参考法律法规与标准清单		
规范类型	实行年份	名称
法律	2007	《中华人民共和国反洗钱法》
	2010	《中华人民共和国保守国家秘密法》
	2012	《全国人民代表大会常务委员会关于加强网络信息保护的决定》
	2012	《中华人民共和国治安管理处罚法（2012 修正）》
	2013	《中华人民共和国消费者权益保护法（2013 修正）》
	2015	《中华人民共和国国家安全法》
	2016	《中华人民共和国网络安全法》
	2017	《中华人民共和国测绘法（2017 修订）》
	2018	《中华人民共和国电子商务法》
	2019	《中华人民共和国密码法》
	2019	《中华人民共和国电子签名法（2019 修正）》
	2019	《中华人民共和国反不正当竞争法（2019 修正）》
	2020	《中华人民共和国民法典》
	2020	《中华人民共和国刑法（2020 修订）》
	2020	《中华人民共和国未成年人保护法（2020 修订）》
	2020	《中华人民共和国著作权法（2020 修正）》
	2020	《中华人民共和国基本医疗卫生与健康促进法》
	2021	《中华人民共和国档案法》
	2021	《中华人民共和国数据安全法》
	2021	《中华人民共和国个人信息保护法》
	2021	《中华人民共和国广告法（2021 修正）》
	2022	《中华人民共和国反垄断法（2022 修正）》
	2022	《中华人民共和国反电信网络诈骗法》
行政法规	1997	《中华人民共和国计算机信息网络国际联网管理暂行规定》
	2011	《计算机信息网络国际联网安全保护管理办法（2011 修订）》
	2013	《信息网络传播权保护条例（2013 修订）》
	2013	《征信业管理条例》
	2019	《中华人民共和国人类遗传资源管理条例》
	2021	《关键信息基础设施安全保护条例》
	2023	《商用密码管理条例》
司法解释	2011	《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》
	2013	《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》
	2017	《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》

		《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》
	2019	《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定（2020 修正）》
	2020	《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定（2020 年修正）》
	2021	《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》
	2022	《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》
	2022	《最高人民法院关于审理网络消费纠纷案件适用法律若干问题的规定（一）》
	2022	《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》
部门规章等规范性文件	2013	《电信和互联网用户个人信息保护规定》
	2018	《银行业金融机构数据治理指引》
	2018	《公安机关互联网安全监督检查规定》
	2018	《检察机关办理侵犯公民个人信息案件指引》
	2018	《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	《国家健康医疗大数据标准、安全和服务管理办法（试行）》
	2019	《互联网个人信息安全保护指南》
	2019	《App 违法违规收集使用个人信息自评估指南》
	2019	《网络信息内容生态治理规定》
	2019	《儿童个人信息网络保护规定》
	2019	《App 违法违规收集使用个人信息行为认定方法》
	2019	《关于开展 App 违法违规收集使用个人信息专项治理的公告》
	2019	《金融信息服务管理规定》
	2020	《中国银保监会监管数据安全管理办法（试行）》
	2020	《中国人民银行金融消费者权益保护实施办法》
	2020	《商业银行互联网贷款管理暂行办法》
	2020	《车联网网络安全和数据安全标准体系建设指南》
	2021	《上海市数据条例》
	2021	《汽车数据安全管理若干规定》
	2021	《关于加强车联网网络安全和数据安全工作的通知》
	2021	《网络安全审查办法》
	2021	《互联网用户公众账号信息服务管理规定（2021 修订）》
	2021	《网络交易监督管理办法》
	2021	《互联网信息服务算法推荐管理规定》
	2021	《科学数据管理办法》
	2021	《关于加强互联网信息服务算法综合治理的指导意见》
	2021	《网络产品安全漏洞管理规定》
	2021	《征信业务管理办法》

	2021	《网络安全审查办法》
	2021	《常见类型移动互联网应用程序必要个人信息范围规定》
	2021	《电信和互联网行业提升网络数据安全保护能力专项行动方案》
	2022	《互联网用户账号信息管理规定》
	2022	《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》
	2022	《工业和信息化领域数据安全管理办法（试行）》
	2022	《数据出境安全评估办法》
	2022	《车联网网络安全和数据安全标准体系建设指南》
	2022	《互联网宗教信息服务管理办法》
	2022	《移动互联网应用程序信息服务管理规定》
	2022	《互联网弹窗信息推送服务管理规定》
	2022	《互联网信息服务深度合成管理规定》
	2022	《数据出境安全评估申报指南（第一版）》
	2022	《关于开展“清朗·2022 年算法综合治理”专项行动的通知》
	2022	《银行保险机构消费者权益保护管理办法》
	2022	《个人信息保护认证实施规则》
	2023	《互联网广告管理办法》
	2023	《证券期货业网络和信息安全管理办法》
	2023	《关于进一步提升移动互联网应用服务能力的通知》
	2023	《个人信息出境标准合同备案指南》
	2023	《个人信息出境标准合同办法》
	2023	《人类遗传资源管理条例实施细则》
	2023	《生成式人工智能服务管理暂行办法》
	2023	《关于规范货币经纪公司数据服务有关事项的通知》
标准	2017	《信息安全技术 移动智能终端个人信息保护技术要求》
	2018	《证券期货业数据分类分级指引》
	2019	《信息安全技术 个人信息去标识化指南》
	2019	《信息安全技术 网络安全等级保护基本要求》
	2019	《信息安全技术 大数据安全管理指南》
	2020	《网络安全标准实践指南-移动互联网应用程序（App）收集使用个人信息自评估指引》
	2020	《个人金融信息保护技术规范》
	2020	《网络安全标准实践指南-移动互联网应用程序（App）中的第三方软件开发工具包（SDK）安全指引》
	2020	《网络安全标准实践指南-移动互联网应用程（App）系统权限申请使用指引》
	2020	《网络安全标准实践指南-移动互联网应用程序（App）个人信息保护常见问题及处置指南》
	2020	《信息安全技术 健康医疗数据安全指南》
	2020	《信息安全技术 个人信息安全规范》
	2020	《基础电信企业数据分类分级方法》
	2020	《电信网和互联网数据安全通用要求》

	2020	《金融数据安全 数据安全分级指南》
	2021	《金融数据安全 数据生命周期安全规范》
	2021	《基础电信企业重要数据识别指南》
	2021	《电信网和互联网数据安全评估规范》
	2021	《信息安全技术 个人信息安全影响评估指南》
	2021	《网络安全标准实践指南——网络数据分类分级指引》
	2021	《产品质量信息系统信息分类与共享交换》
	2021	《个人信息处理法律合规性评估指引》
	2021	《信息安全技术 区块链信息服务安全规范》
	2021	《信息安全技术 恶意软件事件预防和处理指南》
	2021	《信息技术移动设备生物特征识别》
	2022	《合规管理体系 要求及使用指南》
	2022	《信息安全技术 网络数据处理安全要求》
	2022	《信息安全技术 快递物流服务数据安全要求》
	2022	《信息安全技术 移动互联网应用（App）收集个人信息基本要求》
	2022	《信息安全技术 个人信息安全工程指南》
	2022	《信息安全技术 人脸识别数据安全要求》
	2022	《信息安全技术 汽车数据处理安全要求》
	2022	《信息安全技术 基因识别数据安全要求》
	2022	《信息安全技术 声纹识别数据安全要求》
	2022	《信息安全技术 网络数据处理安全要求》
	2022	《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》
	2022	《信息安全技术 网上购物服务数据安全要求》
	2022	《信息安全技术 即时通信服务数据安全要求》
	2022	《互联网广告 匿名化实施指南》
	2023	《信息安全技术 个人信息去标识化效果评估指南》
	2023	《信息安全技术 数据安全评估机构能力要求》
	2023	《智能网联汽车 自动驾驶数据记录系统》
	2023	《信息安全技术 个人信息处理中告知和同意的实施指南》
	2023	《汽车整车信息安全技术要求》
	2023	《信息安全技术 信息安全控制》
	2023	《健康医疗数据合规流通标准》
	2023	《信息安全技术 个人信息跨境传输认证要求》
	2023	《信息安全技术 人工智能计算平台安全框架》
	2023	《信息安全技术 电信领域数据安全指南》