数字经济时代工业企业转型升级的数据合规问题

一、工业企业数据合规的源起

随着数字经济快速发展，数据已成为重要的生产要素，尤其是工业数据是数字经济时代提高企业生产力的关键要素[1]。2019 年 7 月工信部、教育部、人社部等国家十个部、委、局联合下发《加强工业互联网安全工作的指导意见》的通知，主要围绕设备、控制、网络、平台、数据安全等方面，落实企业主体责任、政府监管责任，健全制度机制、建设技术手段、促进产业发展、强化人才培育，构建责任清晰、制度健全、技术先进的工业互联网安全保障体系，覆盖工业互联网规划、建设、运行等全生命周期。

2020 年 4 月 28 日工信部发布《工业和信息化部关于工业大数据发展的指导意见》，旨在促进工业数据汇聚共享、深化数据融合创新、提升数据治理能力、加强数据安全管理，着力打造资源富集、应用繁荣、产业进步、治理有序的工业大数据生态体系。并明确提出构建工业数据安全管理体系，明确企业安全主体责任和各级政府监督管理责任，构建工业数据安全责任体系。加强态势感知、测试评估、预警处置等工业大数据安全能力建设，实现闭环管理，全面保障数据安全。加强工业数据安全产品研发。开展加密传输、访问控制、数据脱敏等安全技术攻

[1] 王伟玲《基于价值链的工业数据治理：模型构建与实践指向》，载《科技管理研究》2020 年第 21 期

关，提升防篡改、防窃取、防泄漏能力。加快培育安全骨干企业，增强数据安全服务，培育良好安全产业生态。

2021 年 11 月 15 日工信部印发《“十四五”大数据产业发展规划》，明确提出优化工业价值链。以制造业数字化转型为引领，构建多层次工业互联网平台，同时还提出，围绕数据全生命周期关键环节，加快数据“大体量”汇聚，强化数据“多样化”处理，推动数据“时效性”流动，加强数据“高质量”治理，促进数据“高价值”转化；筑牢数据安全保障防线，坚持安全与发展并重，加强数据安全管理，加大对重要数据、跨境数据安全的保护力度，提升数据安全风险防范和处置能力，做大做强数据安全产业，加强数据安全产品研发应用等六项重点任务；通过数据安全铸盾行动，加强数据安全管理能力、数据跨境安全管理能力和建设数据安全监测系统。

综上，工业数据合规势在必行，近几年工业互联网的快速发展，其所面临的数据安全挑战与日俱增，工业终端联网程度不断加深，大量工业控制系统、设备设施、数据信息、技术等暴露在互联网上，工业大数据面临传统网络威胁和工业互联网安全风险“双重压力”，安全形势愈发严峻复杂[2]。企业扎实推进数据合规管理工作既是法律政策要求，也是企业长远发展的必然选择。

二、工业企业数据合规的挑战

（一）数据内外部风险

结合公开数据和实践分析我们可以得出，当前工业数据合规面临主要挑战表现为：

[2] 《工业数据安全的合规与防护》，载《工信论坛》2021 年 8 月 21 日

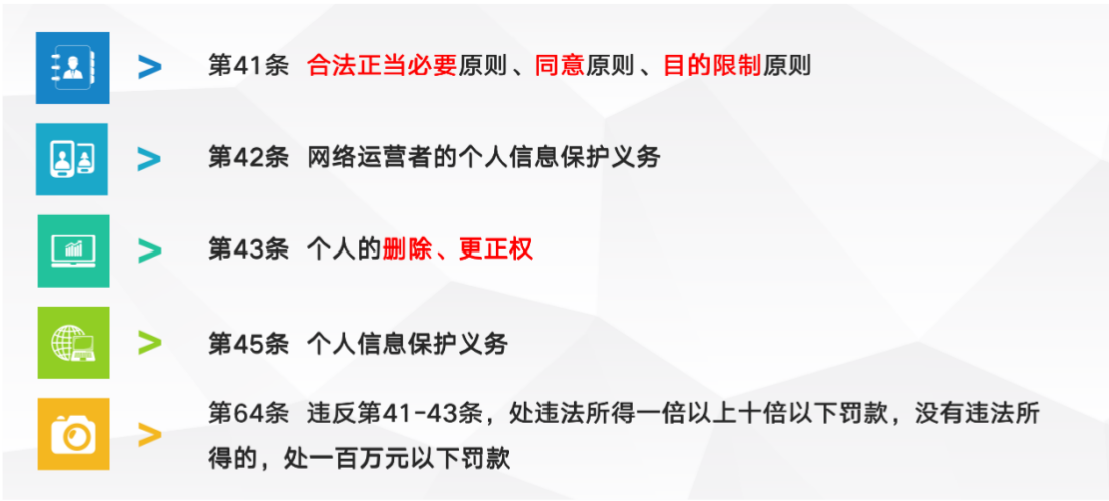
1.数据体量大：中国工业互联网研究院院长徐晓兰接受《每日经济新闻》采访时表示：国家工业互联网大数据中心共连接 41 家工业互联网平台、703 万家企业，数据条目达到 3.43 亿条，云化部署工业 APP 1130 个。工业互联网平台连接设备种类繁多、数据条目数量庞大、涉及企业近千万家，其中关于安全边界的防护、数据分级分类处理、网络安全监管等问题亟待解决。

2.数据质量低：据数据观统计，企业每年因工业大数据质量低下影响数据分析结果而遭受的损失占据其整体收益的 10%-20%。中国数据资产管理发展较晚，中国仅有 30%的工业企业已开展数据治理，近 51%的企业仍沿用文档等原始的数据管理方式，企业数据资产管理意识不强易导致有价值的数据流失，为企业收益带来风险。

3.外部环境恶劣：2021 年 2 月 5 日，国家工业信息安全发展研究中心发布《2020 年工业信息安全态势报告》，报告提及“工业领域因运营成本高、数据价值大、社会影响广成为攻击的首选目标，全年捕获恶意攻击超 200 万次”等内容。所涉及的外部数据风险包括但不限于数据泄露、数据篡改、数据传输、非法访问、流量异常等。

（二）监管压力大

1.《网络安全法》（2016）



2.《数据安全法》（2021）

适用范围	□ 在中华人民共和国境内开展数据处理活动及其安全监管；在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。 □ 数据是指任何以电子或者其他方式对信息的记录。
制度体系	□ 数据分类分级保护、重要数据保护、国家核心数据保护制度 □ 数据安全审查制度 □ 数据出口管制制度 □ 数据安全风险管理和监测预警机制 □ 数据安全应急处置机制
监管部门	□ 中央国家安全领导机构及各地区、各部门行业主管部门（工业、电信、交通、金融、自然资源、卫生健康、教育、科技等） □ 公安机关、国家安全机关等 □ 国务院标准化行政主管部门和国务院有关部门 □ 国家网信部门
保护义务	□ 处理活动应合法正当，符合社会公德和伦理 □ 建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全 □ 利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行数据安全保护义务，并应加强风险监测和事件应急响应 □ 重要数据处理者还应明确数据安全负责人和管理机构，定期开展风险评估并报送报告，依据出境管理规定管理出境活动等
法律责任	□ 责令改正，给予警告 □ 罚款：组织、个人五万元~二百万元；主管、直接负责的主管人员和其他直接责任人员一万元~二十万元，暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照 □ 罚款：违反国家核心数据管理制度，危害国家主权、安全和发展利益的，二百万～一千万元 □ 其他：依法追究刑事责任、依法承担民事责任、依法给予治安管理处罚等

3.《个人信息保护法》（2021）

（一）明确个人信息处理的合法基础

《个人信息保护法》列举了个人信息处理的合法基础包括授权同意、为订立或履行个人作为一方当事人的合同所必需、履职必需、应对突发公共卫生事件、在合理的范围内处理已公开的信息、公益目的等等，总体而言采取了优先保护个人权利和社会公共利益的路径。

（二）为个人赋予撤回同意的权利

考虑到实践中普遍存在的不支持注销账户、撤回同意投诉无门等问题，《个人信息保护法》要求个人信息处理者提供便捷的撤回同意方式。就“便捷”而言，依照相关国家标准的精神，其便捷程度宜与给予授权的便捷程度相对等。

（三）将不满十四周岁未成年人的个人信息列入敏感个人信息

《个保法》明确要求将不满十四周岁未成年人的个人信息作为敏感个人信息加以保护。因此相关数据处理者可能需要更改内部数据分级分类的标准，依照我国法律和相关标准对敏感信息的要求对涉及的不满十四周岁未成年人的个人信息进行特别保护。

（四）针对自动化决策提出明确要求

针对用户画像、“大数据杀熟”等问题，《个人信息保护法》立足于维护广大人民群众的网络空间合法权益，充分吸收了成熟国家标准与行业实践的内容，从算法伦理、数据获取、数据使用、风险评估和日志记录的方面对自动化决策进行了规制。

（五）全面规范个人信息跨境的规则

《个人信息保护法》设置专章对个人信息跨境提供的规则进行了全面的规范，与《数据安全法》《网络安全法》形成了完善的法律体系衔接。

（六）明确个人信息侵权行为的归责原则为过错推定

《个人信息保护法》明确了当个人信息权益因个人信息处理活动受到侵害时，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

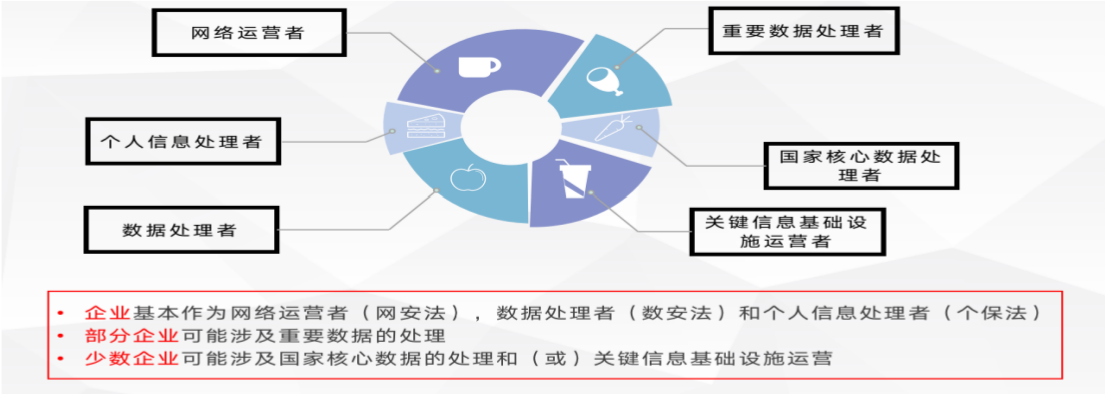
4.相关标准要求

序号	标准名
1	GB/T33132-2016 信息安全技术—信息安全风险处理实施指南
2	GB/T25070-2019 信息安全技术—网络安全等级保护安全设计技术要求
3	GB/T22239-2019 信息安全技术—网络安全等级保护基本要求
4	GB/T28448-2019 信息安全技术—网络安全等级保护测评要求
5	GB/T38672-2020 信息技术 大数据 接口基本要求
6	GB/T38667-2020 信息技术 大数据 数据分类指南
7	GB/T38673-2020 信息技术 大数据 大数据系统基本要求
8	GB/T38676-2020 信息技术 大数据 存储与处理系统功能测试要求
9	GB/T38643-2020 信息技术 大数据 分析系统功能测试要求
10	GB/T38675-2020 信息技术 大数据 计算系统通用要求
11	GB/T38633-2020 信息技术 大数据 系统运维和管理功能要求
12	GB/T39400-2020 工业数据质量—通用技术规范
13	GB/T38666-2020 信息技术 大数据 工业应用参考架构
14	GB/T38555-2020 信息技术 大数据 工业产品核心元数据
……	

（三）企业的多重身份

根据法律及相关文件规定，企业负有的多重身份所带来的责任和义务；当前部分工业企业自身工业数据安全主体责任仍不明确，工业数据安全管理机制存在不同程度的缺失[3]。有关工业数据安全的责任人及职责界定不清，出现问题难以追责，企业管理层缺乏对工业控制系统安全、工业数据合规等的重视。

[3]杨梓涛,王尊《浅谈工业企业工业数据安全保护建议》,载《新型工业化》2021,11(10):141-143



三、工业数据处理过程中的主要风险及解决方案

序号	数据处理环节	风险内容	解决方案
1	收集	工业数据的产生来源众多且数据分布多样，包括设施设备、工业产品、操作系统等。	数据收集过程中，应当采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行书面记录。
2	存储	由于数据量巨大，数据往往需要进行储存，储存时面临数据被超级用户访问、程序攻击、没有被真正隔离等风险。	数据收集后，必须要进行存储，采用云存储技术，建议以多副本、多节点、分布式等的形式存储各类数据；若为第三方存储时建议签署储存协议，可约定存储的时间、地点、管理人、数据备份、数据提取等内容。
3	使用	作为重要的生产要素，在数据上传、查询、访问、下载等活动中，同时在跨系统、跨部门、跨公司、跨国等过程中的数据使用，可能会涉及数据多方存储、权限混乱、泄露等数据风险。	利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制，建立登记、审批机制并留存记录。
4	传输	数据在存储、使用等过程中，都会涉及数据传输，在这过程中可能会失去对数据安全性的控制。	根据传输的数据类型、级别和应用场景，制定法律安全策略并采取保护措施。重要数据的，还应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，涉及跨组织机构或者使用公共信息网络进行数据传输的，应当建立登记、审批机

			制。
5	提供	数据共享可能发生在工厂内部，例如跨部门之间的数据共享，工厂之间的数据共享。这些数据势必被其他部门或者工厂存储，同时也可能会有不同角色的人也可以看到这些数据，势必会增加整个数据泄露的风险。	依据行业数据分类分级管理要求，签署数据服务协议，明确数据提供的范围、数量、条件、程序等。工业和电信数据处理者应当事先对数据接收方的数据安全保护能力进行核实，并与数据接收方签订数据安全协议，明确数据提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任，并督促接收方予以落实。
6	删除	数据在工业数据平台删除不彻底，可能会造成敏感数据泄露。在云环境下，用户失去了对数据的物理存储介质的控制权，无法保证数据存储的副本同时也被删除，导致传统删除方法无法满足大数据安全的要求。	数据处理者应当建立数据删除策略和管理制度，明确删除对象、流程和技术等要求，对销毁活动进行记录和留存。

四、构建工业数据安全战略保障体系

序号	体系设计	具体内容	法律及相关依据
1	进行数据分类分级&制作数据清单	数据分类分级是工业数据合规治理的基础要求；根据《工业数据分类分级指南（试行）》的规定，首先工业企业结合生产制造模式、平台企业结合服务运营模式，分析梳理业务流程和系统设备，考虑行业要求、业务规模、数据复杂程度等实际情况，对工业数据进行分类梳理和标识，形成企业工业数据分类清单。可编写目录进行归档储存；同时针对今后工业数据采集获取的大量数据，进行及时分类分级建立数据清单进行归档储存，形成工业数据资源目录和工业数据资产。其次，可依据不同类别工业数据遭篡改、破坏、泄露或非法利用后，可能对工业生产、经济效益等带来的潜在影响，将工业数据分为一级、二级、三级等3个级别。	《网络安全法》第二十一条；《工业和信息化领域数据安全管理办法（试行）》第七条。
2	企业内部管理制度和操作规范的完善	企业应健全工业数据全流程安全管理制度，涉及到个人信息的还应建立健全个人信息保护合规制度体系，完善内部管理制度和具体操作规程。开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。	《数据安全法》第二十七条、第二十九条；《个人信息保护法》第五十八条。

3	定期开展风险评估	企业应定期开展个人信息保护合规审计以及涉及重要数据的定期开展风险评估，可定期自行开展或委托第三方专业测评机构开展工业数据安全风险评估工作，及时掌握自身工业数据安全风险现状，对评估中发现的问题及时整改，确保自身工业数据满足分类分级保护要求，确保当前采取的安全防护措施切实有效，形成覆盖工业数据全生命周期管理的全方位安全防护机制4。	《个人信息保护法》第五十四条、第六十四条；《数据安全法》第三十条；中国科学技术法学会 T/CLAST 001—2021《个人信息处理法律合规性评估指引》团体标准。
4	企业个人信息安全事前影响评估	针对个人信息的以下情形，企业应开展个人信息安全事前影响评估；且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。 （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； （6）个人信息的处理目的、处理方式等是否合法、正当、必要； （7）对个人权益的影响及安全风险； （8）所采取的保护措施是否合法、有效并与风险程度相适应。	《个人信息保护法》第五十五条、第五十六条；《信息安全技术个人信息安全规范》3.9、11.4。
5	企业个人信息出境	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： （1）依照《个人信息保护法》第四十条的规定通过国家网信部门组织的安全评估； （2）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； （3）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； （4）法律、行政法规或者国家网信部门规定的其他条件。	《个人信息保护法》第三十八条、第三十九条、第四十条、第四十一条；《数据安全法》第三十一条；《个人信息出境安全评估办法》（征求意见稿）。
6	数据安全教育培训	企业应建立数据安全教育培训制度，从公司管理层到具体业务职工，都应纳入培训对象范围，尤其是将数据处理权限、	《数据安全法》第二十七条；《个人信息保护法》第五

[4] 王春晖《构建“以人为本”的个人信息保护法律制度》，载《中国信息安全》2021(05):41-44

		分工、流程、标准等内容进行教育培训。	十一条。
7	数据保护官	企业在处理个人信息达到国家网信部门规定数量的，企业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。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。	《个人信息保护法》第五十二条；《数据安全法》第二十七条；《信息安全技术个人信息安全规范》。
8	突发事件的应对与处理	建立针对突发网络安全事件以及行政检查、处罚等的应对与处理制度。 制定安全事件应急响应预案，当遭受安全威胁导致工业控制系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大； 并逐级报送直至属地省级工业和信息化主管部门，同时注意保护现场，以便进行调查取证； 需要自主或委托第三方工控安全服务单位制定工控安全事件应急响应预案； 预案应包括应急计划的策略和规程、应急计划培训、应急计划测试与演练、应急处理流程、事件监控措施、应急事件报告流程、应急支持资源、应急响应计划等内容。	《工业控制系统信息安全防护指南》

五、总结

通过分析梳理工业数据合规的源起、挑战以及构建工业数据安全战略保障体系的举措，旨在引导工业企业应进一步强化落实自身工业数据安全管理主体责任，贯彻落实《网络安全法》《数据安全法》《个人信息保护法》《工业和信息化领域数据安全管理办法（试行）》《工业和信息化部关于工业大数据发展的指导意见》等相关法律法规和政策文件要求。根据企业自身特点和发展规划，在律师、工程师等人士的协助下，构建起相对完善的工业数据安全战略保障体系。

为此，主要着力点总结如下：明确工业数据安全保护责任人及其岗位职责，明确各岗位在各自职责范围应履行的工业数据安全保护义务和应承担的工业数

据安全保护责任，并在关键岗位开展人才梯度培养计划；设计涵盖工业数据安全的整体方案，包括：数据收集、管理储存、数据使用、流通共享、数据删除、供应链管理、第三方评估、培训教育、问责通报和应急处置等多方面的管理制度；建立健全工业数据分类分级管理、工业数据处理权限管理、工业数据安全合规性评估、工业数据生命周期管理、工业数据关联方管理、工业数据安全应急响应、工业数据跨境合规管理等工业数据管理制度。

附：依据的主要法律法规和其他规定

1.《中华人民共和国网络安全法》

2.《中华人民共和国数据安全法》

3.《中华人民共和国个人信息保护法》

4.《加强工业互联网安全工作的指导意见》

5.《工业和信息化部关于工业大数据发展的指导意见》

6.《“十四五”大数据产业发展规划》

7.《2020 年工业信息安全态势报告》

8.《工业和信息化领域数据安全管理办法（试行）》

9.《个人信息出境安全评估办法》（征求意见稿）

10.《信息安全技术个人信息安全规范》

12.《工业数据分类分级指南（试行）》

13.《工业控制系统信息安全防护指南》

14.《工业数据质量—通用技术规范》（GB/T 39400-2020）

15.《数据管理能力成熟度评估模型》（GB/T 36073-2018）

16.《信息技术 大数据 存储与处理系统功能测试要求》GB/T 38676-2020

17.《信息技术 大数据 工业应用参考架构》GB/T 38666-2020