企业全生命周期数据合规专项管理要点

2022-07-12

大数据、人工智能、云计算等新兴技术推动了数字经济的发展，数据要素已成为引领中国高质量发展的一个新引擎。数据化时代，数据的分布式存储、多渠道流转、多业务共享也使得数据活动场景复杂性增大，新的信息安全风险点日益剧增。

在此背景下，我国的数据安全也迈入了强监管时代。《网络安全法》、《数据安全法》、《个人信息保护法》三大基本数据法陆续出台，立法活动涉及的细分话题与关切要点进一步包括了数字化转型、人工智能、网络内容治理、征信、区块链、移动应用程序、网络交易平台、金融数据安全、智能网联汽车、算法监管、 SDK 管理、网络直播、人脸识别、 CII、数据出境 、地方数据立法等，填补了我国数据安全法律法规的立法空白，构建了我国网络空间治理和数据保护的基本法，对企业的数据收集及使用等各环节，均做出了明确规范和要求。同时，中央及地方层面专项整治行动显著增多在国家政策不断明晰，行业监管持续加强背景下，当前，数据合规的时代已全面到来。如何排除企业数据合规风险，切实做到数据合规，是许多企业亟需解决的问题。

一、正确理解数据合规管理工作及其意义

数据合规的管理是指企业为实现网络安全、数据安全、个人信息及隐私保护这三个合规目标进行的一些列管理活动。从数据处理环节的维度看，数据合规涉及数据收集、使用、共享、传输、披露、存储、删除等通用场景下的合规工作，以及第三方数据处理、数据出境及境外数据处理等特定场景下的合规工作。

对于很多企业来说，数据是公司的核心资产，但很多企业没有数据合规管理意识，往往因被忽略的数据合规风险导致公司发生重大经营风险。2021年，工信部针对违规通报中未按要求完成整改的 App 进行了下架处理，共进行了10 次下架通报，因未按要求完成整改被工信部下架的 App 共 计 342 款。

企业数据合规与安全，成了企业无法回避的话题。随着数字经济的发展，企业通过数据商业化实现对所持有数据资产的变现将在未来为企业创造更为广阔的增值空间。此外，数据合规对于提升企业商业信誉和社会影响力也有着深远意义。

二、科学构建数据合规管理体系——1+3+3+6结构

（一）一个体系架构

数据合规有其特殊性，具有专业性、技术性及多学科融合的特点，因此数据合规管理体系需要在大合规的合规管理体系的架构基础上，加强与产品、业务的关联性，在不同模块上，设计针对数据合规的专项调整。架构模块如下：

模块一：识别风险

基于企业所处的行业及主营业务，结合外部适用的法律法规及内部制定的合规管理制度、签署的相关合作协议、自愿性适用的约定，明确数据合规义务，并结合企业当前的数据合规管理实践，利用风险热力图等风控技术，从影响力和发生频率两个维度评估合规风险，形成动态风险清单。

模块二：审视数据资产

对企业数据资产进行审视，包括数据的来源、类型、访问频率等。对数据资产进行分类，用于评估数据安全风险等级、制定相应的数据合规管理措施等。把控数据在业务中的整个生命周期可能产生的风险。

模块三：布局数据合规管理架构

部署数据合规管理组织架构，明确决策层、执行层与管理层，并明确相关人员的职责。

模块四：制定并完善数据合规管理制度

在数据合规管理架构的基础之上，结合流程，制定相应的数据安全管理措施，完善数据合规管理制度。

模块五：数据合规培训

企业应定期进行数据合规培训，培训对象包括企业员工、第三方合作伙伴等。有能力的企业可以录制合规培训视频，搭建合规培训课程库。同时应注意一线业务部门与中层管理部门之间信息反馈渠道的建设，一线业务部门往往对行业动态更敏感，能够及时反馈最新的信息。

模块六：数据合规监控与审计

企业可根据自己的业务特点及自身发展的阶段性目标，将数据合规完成度、潜在风险等内容数据化，通过建模的方法，对数据合规管理体系的运作情况进行日常监控与审计。

模块七：持续改进

针对数据合规监控与审计的结果，对数据合规管理体系进行改进。

（二）三个负责人

《网络安全法》、《数据安全法》、《个人信息保护法》三部基础性法律均明确规定了指定负责人的情形：

1.网络安全负责人

《网络安全法》规定网络运营者确定网络安全负责人，落实保护责任：关键信息基础设施运营者（ CIIO ）还负有特别责任，应当设置专门安全管理机构和安全管理负责人并对该负责人和关键岗位的人员进行安全背景审查。

2.数据安全负责人

《数据安全法》规定重要数据处理者明确数据安全负责人，成立数据安全管理机构，落实数据安全保护责任。根据2021年1l月14日发布的《网络数据安全管理条例》（征求意见稿），数据安全负责人应当具备数据安全专业知识和相关管理工作经历，由数据处理者决策层成员承担，有权直接向网信部门和主管、监管部门反映数据安全情况。

3.个人信息保护负责人

《个人信息保护法》规定处理个人信息达到一定数量的个人信息处理者，应当指定个人信息保护负责人，对个人信息处理活动以及采取的保护措施等进行监督，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。

（三）三道防线

第一道防线，由业务部门安全与隐私合规工程师构成，主要向业务负责人及安全与合规委员会汇报，负责产品安全隐私策略的具体落地应用、自查自纠等。

第二道防线，由专职的安全隐私部门（含法务、信息安全人员）构成，主要向安全与合规委员会汇报，负责安全隐私能力的建设与支持、推动产品安全隐私策略的落地。

第三道防线，由审计部门担任，主要向安全与合规委会员汇报，负责产品安全隐私策略落地的审计，发现风险并推动业务整改。

（四）六项制度

数据安全管理制度
数据资产管理制度
数据安全事件管理制度
个人信息主体权利相应制度
合作方管理制度
配合执法制度

三、梳理数据合规义务的模块设计及合规风险

企业在完善数据合规义务清单，进行义务识别时，可根据数据处理的环节逐级梳理：

（一）收集

例如，企业在处理敏感个人信息，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、公开个人信息，向境外提供个人信息或实施其他对个人权益有重大影响的个人信息处理活动，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。

（二）存储和跨境传输

例如，如果企业是关键信息基础设施运营者，其在境内运营中收集和产生的个人员息和重要数据应当在境内存储。确需向境外提供的，除另传有规定外，应当根据规定进行安全评估。

（三）使用和加工

例如，企业以个人同意为合法基础处理个人信息，在使用时目的、方式和个人信息的种类发生变化的，应当重新取得个人同意。企业利用个人信息进行自动化决策的，应当事前进行个人信息保护影响评估并留存记录，应当保证决策的透明度和结果公平、公正。

（四）提供或公开

例如，企业因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当履行告知义务。

（五）删除

例如，《电子商务法》第31条规定，“商品和服务信息、交易信息保存时间自交易完成之日起不少于三年。”因此对于电子商务平台经营者来说，交易信息中的个人信息保存期限应不少于三年。出现法律，行政法规规定的法定删除情形时，企业应主动履行删除义务；企业未履行该义务的，个人有权请求企业删除。

企业面临的数据合规风险，则可以从民事责任、行政责任、刑事责任这三个法律责任的维度梳理。有更高合规目标的企业，也可将商誉风险纳入合规风险评估范围内。

1.民事责任

《网络安全法》、《数据安全法》及《个人信息保护法》均规定数据处理主体违反法律规定，给他人造成损害的，须依法承担民事责任。在侵害个人信息权益类案件中，所应遵循的是过错推定原则、损害赔偿数额的认定规则及关于涉个人信息的公益诉讼制度。企业如果不做好数据合规管理，若想自证无过错会面临很大的现实障碍。

2.行政责任

三大基础法均规定了对企业责令改正、警告、罚款、没收违法所得、责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照或类似的行政责任类型。此外，针对企业开展数据处理活动中的高管及第一责任人也有单独的行政处罚措施，对于直接负责的主管人员，除罚款外，还规定了将违法行为被记录到信用档案，乃至职业禁入的处罚措施。

3.刑事责任

非法处理数据还有可能触犯例如侵犯公民个人信息罪、非法侵人计算机信息系统罪、非法获取计算机信息系统数据罪、非法控制计算机信息系统罪提、破坏计算机信息系统罪、拒不履行网络安全管理义务等罪名。对于个人而言，构成上述犯罪的，将有可能被判处有期徒刑、拘役、管制，并处或单处罚金刑。单位实施前述行为，将面临被判处罚金刑的风险，而单位直接负责的主管人员和其他直接责任人员，也将面临有期徒刑、拘役、管制以及并处或单处罚金刑的刑事法律风险。

参考文献：《企业合规事务管理》（高级），企业合规专业委员会组编

附：企业数据合规管理自评表（“是”得1分，不是不得分）

项目		内容	分数
总	数据识别	网络运营者是否已在运营过程中识别数据处理涉及的数据（含个人信息、重要数据和其他数据），形成了数据保护目录并及时更新？	
		网络运营者是否按照相关国家标准与合同、运营的需要，对所识别的数据进行了分类	

体要求	分类分级	网络运营者是否按照相关国家标准与合同、运营的需要，对所识别的数据进行了分类分级管理？		
	风险防控	网络运营者是否建立了数据安全管理责任和评价考核制度？		
		网络运营者是否制定了数据安全保护计划，并定期开展安全风险评估及教育培训？		
	审计追溯	网络运营者是否对数据处理的全生存周期进行了记录？		
安全技术要求	收集	是否制定和公开个人信息保护政策并严格遵守？		
		在收集个人信息前，是否向个人信息主体明示个人信息保护政策并获得其同意？		
		个人信息保护政策中是否明示了提供的产品或服务的类型及所必需的个人信息？		
		当处理个人信息的目的、类型、范围或用途等发生改变时，是否及时修改个人信息保护政策？		
		修改个人信息保护政策后，是否重新征得了个人信息主体的同意？		
		是否因用户不同意或撤回同意提供该产品或服务所必需的个人信息以外的信息而拒绝向用户提供该产品或服务？		
		是否采取措施防止仅以“改善服务质量、提升用户体验、定向推送信息、研发新产品”等目的，强烈要求、误导用户同意收集个人信息？		
		在收集敏感个人信息前，是否取得了个人信息主体的单独同意？该同意是否是在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示？		
		收集不满十四周岁的未成年人个人信息前，是否取得了未成年人的父母或者其他监护人的单独同意？		
		如从个人信息主体以外的其他途径获得个人信息的，是否知晓个人信息来源及个人信息提供方已获得的个人信息处理授权同意范围，并按照《个人信息保护法》《信息安全技术 网络数据处理安全要求》（G B/T 41479-2022）等法律规范的要求履行安全保护义务？		
	存储	网络运营者是否对数据存储活动采取了如下安全措施：		
		1	针对重要数据和个人信息等敏感数据，采用加密、安全存储、访问控制、安全审计等安全措施；	
		2	是否按照重要数据和个人信息主体约定的存储期限或个人信息主体授权同意的有效期存储重要数据和个人信息；	
		3	存储个人生物特征识别信息的，是否遵守 GB /T 35273-2020 中的要求及生物特征识别信息保护相关国家标准要求？	
		4	数据接收方存储数据时，是否按照要求采取安全措施并以合同进行约定？	
	使用	网络运营者在为用户提供定向推送或信息合成服务时，是否遵守了如下要求：		
		1	利用个人信息和算法为用户提供定向推送信息服务的，同时提供了非定向推送信息的服务选项；	
		2	在提供定向推送服务时，显著区分定向推送和非定向推送的内容（如标明“定推”等字样）；	
		3	在提供定向推送服务时，是否向用户提供选择或者删除用于该服务的针对其个人特征的用户标签的功能；	
		4	在向个人信息主体提供新闻、博客类信息服务的过程中，如果利用算法自动合成文字、图片、音视频等信息，是否明确告知用户该情况？	
		网络运营者所提供的产品或服务中如果接入或者嵌入了第三方应用的，是否遵守了如下要求：		
		1	通过合同等形式明确双方的数据安全保护责任和义务；	
			监督第三方应用运营者加强数据安全管理，如发现第三方应用没有落实安全管	

	2	理责任的，及时督促其整改，并在必要时停止接入；	
	3	是否对接入或嵌入的第三方应用开展技术检测，以确保其数据处理行为符合双方约定要求？如在审计过程中发现超出双方约定的行为时是否及时停止接入？	
	网络运营者在开展数据加工活动的过程中，如知道或者应知道可能危害国家安全、公共安全、经济安全和社会稳定的，是否立即停止加工活动？		
	网络运营者在数据传输活动中是否采取如下安全措施：		
	1	在传输重要数据和个人敏感信息时，采取加密、脱敏等安全措施；	
	2	向数据接收方传输数据时，按照法律要求采取安全措施并以合同进行约定？	
向他人提供	网络运营者向他人提供数据前，是否遵守如下要求：		
	1	向个人信息主体告知接受方的名称、联系方式、处理目的、处理方式、个人信息的种类、存储期限，并取得个人信息主体的同意；	
	2	共享、转让重要数据时，与数据接受方通过合同等形式明确双方的数据安全保护责任和义务，并采取加密、脱敏等措施保障重要数据安全；	
	3	委托第三方开展数据处理活动时，通过合同等形式明确约定委托处理的目的、期限、处理方式等双方的权利义务？	
数据出境	网络运营者向境外提供个人信息或者重要数据的，是否遵守《网络安全法》《数据安全法》及《个人信息保护法》等国家相关规定和相关标准的要求？		
	网络运营者的境内用户在境内访问境内网络的，是否采取措施防止该流量路由至境外？		
数据公开	网络运营者在利用所掌握的数据资源进行公开市场预测、统计信息时，是否存在危害国家安全、公共安全、经济安全和社会稳定的可能性？		
私人信息和可转发信息	即时通信等社交平台运营者是否向用户提供私人信息和可转发信息的选项？		
	社交平台运营者对私人选项发送的信息是否给予严格保护，且不提供转发功能？		
	对于以可转发选项发送的信息，或在转发此类信息时，社交平台运营者是否同时发送信息始发者在该平台上的账号名称，同时确保该账号名称唯一且不可更改？		
个人信息查、更正、删除及用户账号注销	是否建立能够及时响应个人信息主体查阅、复制、更正、删除其个人信息及注销账号请求的渠道和机制？		
	如决定不响应个人信息主体的请求，是否向个人信息主体告知该决定的理由，并向个人信息主体提供投诉的途径？		
投诉、举报受理处置	网络运营者是否建立投诉、举报受理处置制度？		
	网络运营者是否能在接受投诉举报起 3 天内受理？		
	网络运营者对于查实的投诉举报，是否能依法采取停止传输、消除等处理措施？		
访问控制与审计	网络运营者开展数据处理活动时，是否遵守如下要求：		
	1	基于数据分类登记，明确相关人员的访问权限，以防止非授权访问；	
	2	是否针对重要数据、个人信息的关键操作（如批量修改、拷贝、删除、下载）设置内部审批和审计流程并严格执行？	
数据删除和匿名化处理	网络运营者是否在下述情况中对个人信息进行删除或匿名化处理：		
	1	个人信息超出双方约定的存储期限时；	
	2	网络产品和服务停止运营时；	
	3	个人信息主体注销账号，或者用户撤回同意时？	
	网络运营者在对存储重要数据和个人信息的介质进行报废处理时，是否采用物理损毁等方式销毁介质，以确保重要数据和个人信息不能被恢复？		
	如果网络运营者在开展经营和服务活动过程中，需处理重要数据和敏感信息的，是		

安全管理要求	数据安全负责人	如果网络运营者在开展经营和服务活动过程中，需处理重要数据和敏感信息的，是否指定数据安全责任人？		
		是否要求数据安全责任人履行以下职责：		
		1	组织确定数据保护目录，制定数据安全保护计划并督促落实；	
		2	组织开展数据安全影响分析和风险评估，督促整改安全隐患；	
		3	依法向有关部门报告数据安全保护和事件处置情况；	
		4	组织受理和处置数据安全投诉、举报？	
	人力资源保障与考核	网络运营者是否明确数据安全保护岗位及职责，并提供人力资源保障？		
		是否建立人力资源考核制度及数据安全管理考核指标和问责机制？		
	事件应急处置	应急响应机制是否包含如下模块：		
		1	数据安全事件分级；	
		2	启动条件；	
		3	启动所需的资源（人员、设备、场所、工具、资金等）；	
		4	流程、人员安排和操作手册？	
		5	是否已经配齐应急响应所需的资源以确保应急响应机制能够有效实施？	
		6	是否已经制定应急演练计划并开展演练？	

来源：

作者：肖琳