数据合规指南

一、中国、欧盟、美国数据合规重点规则[1]

1. 中国数据保护法律重点规定

（1）《中华人民共和国网络安全法》

网络运营者的安全保护义务：包括制定内部安全管理制度、采取技术措施防范网络攻击、监测网络运行状态、采取数据分类、重要数据备份和加密措施等，以保障网络免受干扰、破坏或未经授权的访问，并防止网络数据泄露或被窃取、篡改。

网络安全事件的应对与处置：网络运营者应当制定网络安全事件应急预案，及时防范、发现和应对系统漏洞、计算机病毒、网络攻击等安全风险，并在发生危害网络安全的事件时立即启动应急预案，采取相应补救措施，并按规定向相关主管部门报告。

个人信息保护：网络产品、服务的提供者应当明确告知用户其收集、使用个人信息的目的、方式和范围，并征得用户同意。同时，网络运营者应当采取技术措施和其他必要措施，确保收集的个人信息安全，防止信息泄露、毁损或丢失。

法律责任：对于不履行网络安全保护义务、违反个人信息保护规定等行为，相关主管部门将责令改正并给予警告或罚款等行政处罚。对于构成犯罪的行为，将依法追究刑事责任。

（2）《中华人民共和国数据安全法》

数据保护的域外法律效力：损害国家安全、公共利益或公民、组织合法权益

的数据处理活动，都将依法追究法律责任。

数据安全与发展：该法强调在保障数据安全的基础上促进数据的开发利用，明确了数据安全与发展的关系，并提出了相应的措施来促进数据开发利用和技术研究应用。

数据安全监管机制：国家建立了数据安全应急处置机制和审查制度，对影响或可能影响国家安全的数据处理活动进行国家安全审查。此外，还实施了出口管制措施，对关键信息基础设施运营者的重要数据出境安全管理进行了规定。

数据安全保护义务：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，采取相应的技术措施和其他必要措施保障数据安全。重要数据的处理者需明确数据安全负责人和管理机构，落实数据安全保护责任。

关键信息基础设施的运营者：在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者的重的数据出境安全管理办法由国家网信部门会同国务院有关部门制定。

（3）《中华人民共和国个人信息保护法》

个人数据及敏感个人信息定义：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等，以及不满十四周岁未成年人的个人信息。

数据主体权利：知情同意权、查阅、访问与复制权、更正权、删除权、撤回同意权、限制处理权、可携带权、反对权、自动化决策和分析权、投诉权等。

数据处理者义务：采取措施确保个人信息处理活动合规；指定个人信息保护负责人进行监督；定期对其处理个人信息情况进行合规审计；进行个人信息保护影响评估，并对处理情况进行记录；对个人信息泄露、篡改、丢失立即采取补救措施，并履行通知义务；提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者应履行的义务。

数据处理原则：通过自动化决策方式向个人进行信息推送、商业营销时，应提供不针对其个人特征的选项或提供便捷的拒绝方式；处理个人信息要遵循合法、正当、必要和诚信原则、目的限制原则、公开、透明原则、质量原则以及责任与安全原则；处理敏感个人信息，如生物识别、医疗健康、金融账户、行踪轨迹等，应取得个人的单独同意；对于违法处理个人信息的应用程序，法律规定可以责令暂停或终止提供服务。

数据处理的合法正当理由：取得个人的同意；为订立、履行个人作为一方当事人的合同所必需，或者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人力资源管理所必需；为履行法定职责或者法定义务所必需；为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息。法律、行政法规规定的其他情形。

本地化存储要求：关键信息基础设施境内运营过程中产生的个人数据和重要

数据实施数据本地化的要求。

数据跨境传输规则：属于关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，需就其向境外提供个人信息办理了网信部门组织的安全评估；属于经国家网信部门的规定经专业机构进行了个人信息保护认证即可出境的情形，需按照规定进行个人信息保护认证；属于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即可出境的情形，需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；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本法规定权利的方式和程序等事项。

2. 欧盟 GDPR 重点规定

欧盟《通用数据保护条例》General Data Protection Regulation，GDPR）于 2018 年 5 月 25 日正式生效。GDPR 的适用范围广泛，适用于所有位于欧洲经济区的数据控制者和处理者。此外，也适用于以下三种位于欧洲经济区之外的主体：定期向欧洲经济区居民提供商品和服务的企业；定期监控欧洲经济区居民活动的企业（例如使用跟踪 cookie）；代表欧洲经济区控制者处理数据的企业。国家安全或执法活动以及纯粹的个人数据使用不受 GDPR 管辖。

（1）数据跨境

GDPR 规定了欧盟个人数据跨境的三种途径。

其一，是获得“充分性认定”。当欧盟委员会决定第三方已经确定达到充分的保护标准时，数据便可以向第三方转移，而无需经过任何特别授权程序（第三方白名单国家）。由于欧盟的充分性认定较为全面与严格，自瑞士成为首个获得

充分性认定的第三方以来，20 余年间仅有十余个第三方通过欧盟的充分性认定。

其二，为欧盟境内数据主体提供“适当保障措施”。当数据出境的目的地没有获得欧盟的充分性认定时，数据控制者或处理者只有在提供了适当的保障措施并且满足数据主体能行使权利、能获得有效的法律救济的条件时，欧盟境内主体才能将相关个人数据向第三国或国际组织转移。这些保障措施包括：政府间签订有法律约束力和可执行性的文书、有约束力的公司规则等。

其三，特定情况下的豁免。在充分性认定和适当保障措施均不能满足的情况下，数据跨境需求方还可以退而求其次，判断其数据跨境传输是否属于特定情况下的豁免，GDPR 规定了多种豁免情形，如数据主体在被告知该转移行为由于缺乏充分的保护标准和适当的保护措施可能会对其带来的风险后仍明确同意转移。

（2）个人数据保护

GDPR 非常重视个人数据保护。GDPR 将个人数据定义为与可识别人员相关的任何信息，包括直接和间接标识符。直接标识符是指一个人的唯一数据点，例如姓名或信用卡号。间接标识符包括可以识别一个人的非独特特征，例如 Cookie 标识符、IP 地址、外形特征、出生日期等。GDPR 还对敏感个人数据给予更大保护力度，包括以下信息：族裔或种族、宗教信仰、生物识别数据、政治观点、遗传数据、健康信息、性取向或性生活、工会会员身份。敏感数据需要接受更为严格的保护，是因为对这些数据的处理会大大增加个人权利和自由方面所面临风险的可能性和严重性。

只有满足如下条件中的至少一项，对于个人敏感数据的处理才是合法的：数据主体已经明确同意基于一项或多项目的而对其个人数据进行处理；处理对于控

制者履行责任以及行使其特定权利是必要的，或者对于在雇佣、社会安全与社会保障法领域采取符合欧盟或成员国法律或集体协议的措施以保护数据主体的根本权利或利益是必要的；数据主体因身体原因或法律原因而无法表达同意，但处理对于保护数据主体或另一个自然人的核心利益所必要的；基金、协会或者其它具有政治、哲学、宗教或工会目的的非营利机构的正当性活动中所进行的处理，并且已经采取了恰当的保护措施；对数据主体明显已经公开的相关个人数据的处理；当处理对于提起、行使或辩护法律性主张必要；处理对实现实质性的公共利益是必要的；处理对于预防性医学或者临床医学目的是必要的；在公共健康领域，处理是为了实现公共利益所必要的；对于实现公共利益、科学或历史研究目的或统计目的是必要的，处理采取了与其期望目的所相称的处理，并且对数据主体的基本权利与利益采取了合适与特定的措施。

3. 美国数据合规相关规定

《联邦贸易委员会法》（Federal Trade Commission Act, FTC Act）第 5 条是美国数据隐私与安全监管的重要依据。该条款禁止任何“欺骗性或不正当的商业行为”。在数据隐私领域，如果企业对外宣称具备某种隐私保护措施、数据用途限制或不与第三方共享数据，但实际行为与之不符，即构成欺骗性行为，违反该条规定；即便无虚假承诺，若企业未采取合理安全措施而导致数据泄露，也可被认定为不正当行为。联邦贸易委员会（FTC）可基于该条对企业展开执法调查，签发强制命令或同意令，要求企业建立数据保护机制并接受持续监督。

在州法层面，加利福尼亚州于 2018 年通过《加州消费者隐私法案》（California Consumer Privacy Act, CCPA）并于 2020 年生效。CCPA 适

用于满足特定门槛的企业，包括年营业额超过 2500 万美元、每年处理超过 5 万名加州居民个人信息，或 50%以上收入来源于出售个人信息者。CCPA 规定企业必须在信息收集时披露信息种类和用途，并赋予消费者五项权利：知情权、访问权、删除权、选择退出权（opt-out）、非歧视权。企业还需在网站显著位置提供“Do Not Sell My Personal Information”链接，接受消费者拒绝出售其信息的请求，并在规定期限内处理消费者的访问和删除请求。

2020 年通过的《加州隐私权法案》California Privacy Rights Act, CPRA）对 CCPA 进行了扩展和修正并于 2023 年生效。CPRA 引入“敏感个人信息”类别，如社会保障号、种族、健康信息、精准地理位置等，并要求企业提供限制处理该类信息的选项；明确了“数据最小化”和“目的限制”原则，即企业只能为特定且必要目的收集和使用个人数据；要求企业在隐私政策中披露数据保留期限或保留标准；规定企业与第三方、服务提供商、承包商签订合同，约定数据用途、安全义务与用户权利保障。CPRA 还设立加州隐私保护局（California Privacy Protection Agency），专责执法与规范解释。

此外，《美国数据隐私与保护法案》（American Data Privacy and Protection Act, ADPPA）已于 2022 年在国会提出，尚未生效。草案内容包括适用“数据最小化”原则、设置访问、更正、删除等个人权利，并对大型数据处理者提出影响评估要求。若立法通过，将成为美国全国统一的数据保护法规基础。

在个人数据保护义务方面，企业必须向消费者披露他们所收集的个人数据的类型和用途；必须采取适当的安全措施来保护个人数据；必须对个人数据的保护负责；只能收集必要的个人数据；必须确定个人数据的保留期限；必须确保个人

数据的传输安全；必须确保个人数据的存储安全；必须控制个人数据的访问；必须在合同中包括个人数据保护条款;必须确定数据保护义务;必须确定违约责任。消费者有权选择是否允许企业收集和使用他们的个人数据;消费者有权访问和更正他们的个人数据。

二、常见问题与主要风险

1. 告知与同意义务履行不充分

隐私政策信息披露不足：部分企业未能以清晰、易懂的语言向用户披露数据处理的基本要素，如处理目的、方式、范围、保存期限、接收方等，或仅以笼统条款模糊披露。语言版本不一致或不完整：对于跨境运营的产品，仅提供外文版本隐私政策，未提供中文版本。合法性基础不明：未说明个人信息处理所依据的合法性基础（如履行合同、法定义务、用户同意、公共利益等），无法满足合法、正当、必要原则。同意机制不合规：存在强制捆绑同意、默认勾选、一次性笼统授权等做法，妨碍用户自主选择和撤回同意的权利。

2. 数据处理方式存在不当行为

数据最小化原则落实不到位：企业存在采集与其产品或服务无直接关联的过度信息收集行为，如访问剪贴板、相册、联系人、位置等，违反“最少必要”原则。超范围使用与共享个人信息：部分企业将收集信息用于广告推送、商业合作等超出原处理目的的用途，或共享给第三方未充分告知用户。未履行删除义务：用户注销账户后，企业仍保留其个人数据，或无法提供有效的数据删除路径。

3. Cookie 及网络追踪技术使用不合规

使用 Cookie 无明示同意：部分网站或 App 在未明确征得用户同意的情况下设置或使用 Cookie，尤其是广告或分析类 Cookie，违反用户知情同意义务。使用其他追踪技术滥用用户行为数据：如通过 URL 参数、设备指纹等手段跟踪用户跨平台行为，且未说明目的及范围，构成隐性收集。不提供退出机制：用户无法控制或关闭追踪设置，缺乏 Cookie 管理面板或选择退出的机制。

4. 数据跨境传输风险

未履行出境评估或申报义务：企业将数据传输至境外但未履行安全评估、签署标准合同、认证等法定程序。接收国数据保护水平不足：如传输至未被中国网信办认定为“具有充分数据保护水平”的国家，存在个人信息可能被不当访问或使用的风险。集团内部数据传输架构不清：母子公司、境外分支机构间频繁数据传输，权限、边界与接入机制未建立规范制度。

5. 数据主体权利响应机制缺失

无法有效行使个人信息权利：用户请求访问、更正、删除其个人数据时，企业响应不及时或设置高门槛（如附加证明材料、不开放平台通道）。投诉举报机制形同虚设：部分企业未提供用户申诉或投诉入口，或未指定数据保护负责人/联系人。对法律适用范围理解模糊：企业混淆海外用户与中国用户适用标准，导致在处理中国境内数据时未遵循相关标准。

6. 未成年人数据处理存在合规空白

缺乏年龄验证机制：部分产品允许未成年人注册使用但未建立年龄识别与验证手段。未取得监护人明示同意：处理 14 岁以下未成年人信息时，未征得其监护人同意，或未提供监护人撤回同意的渠道。内容引导性不足：隐私政策未单独

列示未成年人数据处理章节，未采取差异化保护措施。

7. 数据安全管理措施不到位

内部权限管理缺失：对数据访问权限控制粗放，存在“超权限访问”“账号共用”“开发测试混用”等问题。数据存储机制不安全：存储位置、方式、加密机制不透明，甚至使用明文存储、共享硬盘、公共云未隔离等方式，带来极高泄露风险。安全事件响应机制缺位：未建立数据泄露通报制度、应急响应预案或备案机制，发现数据安全事件后不能及时处置。技术更新管理混乱：部分企业未建立固件或软件安全升级通道，设备被发现漏洞后长时间不予修复。

8. 人工智能处理中的透明度不足

算法使用未披露：企业在用户画像、个性化推荐、信用评估等环节使用 AI 算法处理个人数据，但未说明处理逻辑、对个人权利影响或解释依据。黑箱模型缺乏可解释性：人工智能模型处理结果无法向用户说明依据，造成“算法歧视”或“算法操控”风险，违反透明原则。

三、企业合规建议[2]

1. 业务场景下的同意管理

基于同意作为数据处理合法性基础的前提，在收集用户数据前，是否以明示、清晰的方式获取了用户的同意是最易感知的、易引发用户关注及投诉的个人信息收集问题。通常情况下，以下数据收集情景，企业应特别留意：（1）应设立隐私政策等明确的个人信息收集处理规则；（2）应以醒目、显著、易于察觉的方式呈现隐私政策（例如使用弹窗、明显的选择框等），方便用户查阅或获得用户

的清晰同意；（3）隐私政策内容需要详实，真实明示产品和服务所涉及的收集和处理的数据类型、数据共享和数据跨境的情况。

此外，数据收集也可能隐藏在私域流量运营等典型情境中，例如在即时通讯应用的群组聊天或评论中。在平台提供的隐私政策之外，企业应结合平台特点，在实施具体数据收集处理活动之前，通过友好的提示或对用户友好的设计，引导用户仔细阅读个人信息收集处理规则，了解并同意规则内容，以确保数据收集场景的合法性。

2. 定向营销

定向营销场景依赖于对个人数据的收集和分析，以精准地针对特定用户进行广告投放，需要确保决策过程的透明度和结果的公正性，以降低合规风险并保护用户权益，应满足的合规要求如下：（1）用户同意和知情权：收集用户数据前，必须以明确、透明的方式告知用户数据将如何使用，并获得他们的明示同意。用户应该清楚了解他们的数据是否将用于定向广告；（2）退出和选择权：用户应具备随时退出定向广告或选择不接收个性化广告的权利，并且这些选项应该易于实现。当用户明确表示拒绝接收个性化推荐时，不得再继续向其发送商业性信息。对于采用自动化决策方式进行商业营销的情况，应同时提供不基于个人特征的选项；（3）数据最小化原则：企业应仅收集为实现定向营销目标所必需的数据，而不是过度收集用户信息，以降低潜在的隐私风险；（4）个人信息的匿名化和去标识化：在将个人数据用于定向广告时，最好使用匿名化和去标识化技术，以降低用户被识别的风险。

3. 第三方数据共享

企业在使用数据的过程中，可能涉及与物流供应商、支付服务提供商、第三方平台供应商等第三方进行数据共享，对其中涉及的大量隐私合规风险，应采取足够的组织和技术措施进行管控。应重点关注的领域包括：（1）识别角色并明确义务：识别企业和第三方的数据处理角色，明确双方在数据保护方面的权利和义务；（2）明确数据使用的目的：为避免数据被滥用，要确保合同中明确定义了共享数据的使用目的，并限制第三方只能按照这些明确的目的使用数据；（3）授权和知情权：透明地向数据主体提供共享细节是合规的关键，要确保数据主体已明确同意数据共享，并清楚了解他们的数据将与哪些第三方共享；（4）数据安全保护：确保第三方有足够的安全措施来保护共享的数据，包括数据传输和存储的加密、访问控制、漏洞修复等；（5）监管和审计：建立监管机制，允许企业对第三方的数据使用情况及数据安全措施的有效性等进行定期审计以确保合规性。

4. 数据安全

企业往往在多个环节都涉及数据合规风险，如源自企业内部的信息泄露、供应商的系统漏洞以及针对用户的钓鱼攻击、账号被盗和木马病毒侵入等，企业必须全面关注并解决这些来自不同环节的数据安全问题，采取合适的措施以保护用户和企业的数据安全。

参考信息：

1.部分内容参考 IBM（中国）有限公司：《企业出海数据合规指导书》。

2.中华人民共和国商务部中国外经贸企业服务网：《跨境电商数据合规要点提示》，2024 年 7 月 31 日。http://12335.mofcom.gov.cn/article/wmzhfwxzyqysj/202407/1940147_1.html