（2025 年 11 月）

目录

一、法规速递

《大型网络平台个人信息保护规定（征求意见稿）》

发文机关：国家互联网信息办公室,公安部

发布时间：2025.11.22

生效时间：待定

第一条 为规范大型网络平台个人信息处理活动，保护个人信息合法权益，促进个人信息依法合理利用，根据《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《中华人民共和国网络安全法》《网络数据安全管理条例》等法律法规，制定本规定。

第二条 在中华人民共和国境内建设、运营的大型网络平台的个人信息保护，适用本规定。法律、行政法规另有规定的，从其规定。

第三条 国家网信部门会同国务院公安部门等有关部门制定发布大型网络平台目录并动态更新。

对大型网络平台的认定，主要考虑以下因素：

（一）注册用户 5000 万以上或者月活跃用户 1000 万以上；

（二）提供重要网络服务或者经营范围涵盖多个类型业务；

（三）掌握处理的数据一旦被泄露、篡改、损毁，对国家安全、经济运行、国计民生等具有重要影响；

（四）国家网信部门、国务院公安部门规定的其他情形。

第四条 提供大型网络平台服务的网络数据处理者（以下简称大型网络平台服务提供者）开展个人信息处理活动，应当遵循合法、正当、必要和诚信原则，遵守法律、法规，遵守社会公德和伦理，对所处理的个人信息安全承担主体责任，严格保护敏感个人

信息和未成年人个人信息，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第五条 大型网络平台服务提供者应当按照法律法规有关规定指定个人信息保护负责人，并公开个人信息保护负责人的联系方式。

个人信息保护负责人应当由大型网络平台服务提供者管理层成员担任，具有中华人民共和国国籍，无境外永久居留权或者长期居留许可，具备个人信息保护专业知识且从事相关工作 5 年以上。个人信息保护负责人可以由网络数据安全负责人兼任。

个人信息保护负责人应当履行下列职责：

（一）指导大型网络平台合规开展个人信息处理活动，落实国家网信部门、国务院公安部门和有关主管部门的个人信息保护监管要求，配合有关部门开展个人信息保护监督检查；

（二）参与大型网络平台个人信息处理事项相关决策，并对个人信息处理事项具有否决权；

（三）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，发现大型网络平台个人信息处理活动存在较大安全风险或者存在违法违规情形的，应当立即采取措施，并向国家网信部门和有关主管部门报告，涉嫌违法犯罪的应当向公安机关报案；

（四）组织制定专门的未成年人个人信息处理规则。

个人信息保护负责人可以直接向国家网信部门、有关主管部门报告大型网络平台服务提供者的个人信息保护有关情况。

第六条 大型网络平台服务提供者应当明确个人信息保护工作机构，在个人信息保护负责人领导下开展个人信息保护相关工作，包括但不限于：

（一）制定实施内部个人信息保护管理制度、操作规程以及个人信息安全事件应急预案，合理确定个人信息处理的操作权限，对大型网络平台的个人信息处理活动进行安全管理；

（二）组织开展个人信息安全风险监测、风险评估、合规审计、影响评估、应急演练、宣传教育培训等活动，及时处置个人信息安全风险和事件；

（三）明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务，

并对其个人信息处理活动和履行个人信息保护义务情况进行监督；

（四）明确专人负责未成年人个人信息保护工作；

（五）受理并处理个人信息保护投诉、举报；

（六）每年编制发布大型网络平台服务提供者个人信息保护社会责任报告。

鼓励大型网络平台服务提供者设立专门的个人信息保护工作机构。

第七条 大型网络平台服务提供者应当为个人信息保护负责人、个人信息保护工作机构履行职责提供必要支持。

第八条 大型网络平台服务提供者应当及时向国家网信部门报送下列信息：

（一）个人信息保护负责人基本信息；

（二）个人信息保护工作机构基本信息；

（三）保障个人信息保护负责人和个人信息保护工作机构履职的措施。

个人信息保护负责人、个人信息保护工作机构等发生变化的，大型网络平台服务提供者应当在 20 个工作日内报送变更信息。

国家网信部门将大型网络平台服务提供者信息向国务院公安部门和有关主管部门共享。

第九条 大型网络平台服务提供者应当将在中华人民共和国境内运营中收集和产生的个人信息存储在境内。确需向境外提供的，应当符合国家数据出境安全管理有关规定。

大型网络平台服务提供者应当按照国家有关规定，健全个人信息出境安全相关技术和管理措施，及时防范、处置个人信息违法违规出境安全风险和威胁。

第十条 大型网络平台服务提供者应当将在中华人民共和国境内运营中收集和产生的个人信息存储在符合下列条件的数据中心：

（一）设立在中华人民共和国境内；

（二）主要负责人具有中华人民共和国国籍，无境外永久居留权或者长期居留许可；

（三）安全性符合国家有关标准要求。

第十一条 数据中心应当协助大型网络平台服务提供者履行个人信息保护义务，包括但不限于：

（一）建立健全内部个人信息管理制度和操作规程；

（二）发现系统、网络产品和服务等存在影响大型网络平台服务提供者履行个人信息保护义务的安全缺陷、漏洞等风险的，应当立即采取补救措施，按照规定向有关主管部门报告，并通报大型网络平台服务提供者个人信息保护负责人；

（三）发生个人信息安全事件时，应当立即通报大型网络平台服务提供者个人信息保护负责人，及时启动应急处置预案，采取措施防止危害扩大，消除安全隐患，并按照规定向国家网信部门、有关主管部门报告；

（四）及时执行国家网信部门、国务院公安部门和有关主管部门个人信息安全保护有关要求。

第十二条 大型网络平台服务提供者委托符合本规定第十条要求的第三方数据中心存储个人信息的，应当与其签订合同，约定存储地点、规模、种类等，明确履行本规定第十一条安全要求和下列职责：

（一）严格依照法律法规的规定和合同约定，履行个人信息保护义务，提供安全、稳定、持续的服务，并接受大型网络平台服务提供者个人信息保护负责人、个人信息保护监督委员会等的监督；

（二）为大型网络平台服务提供者处理个人信息提供便利措施；

（三）协助大型网络平台服务提供者对个人信息处理活动进行安全管理。

第十三条 大型网络平台服务提供者应当向国家网信部门等有关部门报送存储个人信息的数据中心的基本信息，包括管理团队和管理架构、内部个人信息保护管理制度、采取的安全措施、与第三方数据中心签署的合同文本等。上述信息发生变化的，应当自变化之日起 10 个工作日内报送变更信息。

第十四条 大型网络平台服务提供者应当为个人行使查阅、复制、更正、补充、删除、限制处理其个人信息，或者注销账号、撤回同意等权利提供便捷的方法和途径。

个人请求将其个人信息转移至其指定的个人信息处理者的，大型网络平台服务提供者应当在接到个人请求后 30 个工作日内将个人信息通过通用、机器可读的格式进行转移，并以邮件、电话、短信等方式告知个人处理结果，不符合法律、行政法规规定条件的，应当向个人说明原因。因请求数量、操作复杂等原因需要延长处理期限的，应当向个人说明延期原因，可以在合理、必要的情况下再延长 30 个工作日。法律、行政法规、

部门规章另有规定的，从其规定。

支持大型网络平台服务提供者通过应用程序接口或者其他标准化技术方式提供转移途径，采取身份验证、加密传输等安全措施保障个人信息转移安全。

个人重复转移个人信息的，大型网络平台服务提供者可以根据转移个人信息的成本收取必要费用。

第十五条 大型网络平台服务提供者应当按照国家有关规定自行或者委托第三方专业机构开展个人信息保护合规审计、风险评估等活动，并对发现的问题进行整改。鼓励大型网络平台服务提供者优先选择通过认证的第三方专业机构。专业机构的认证按照《中华人民共和国认证认可条例》的有关规定执行。

第十六条 受大型网络平台服务提供者委托开展个人信息保护合规审计、风险评估等活动的第三方专业机构，应当注册在中华人民共和国境内，发现大型网络平台服务提供者的个人信息处理活动存在较大安全风险或者存在违法违规情形的，可以直接向国家网信部门和有关主管部门报告；涉嫌违法犯罪的应当向公安机关报案。

第十七条 大型网络平台服务提供者有以下情形之一的，国家网信部门、国务院公安部门和有关主管部门可以要求其委托第三方专业机构对其个人信息处理活动开展合规审计、风险评估等活动：

（一）个人信息处理活动存在严重影响个人权益或者严重缺乏安全措施等情形的；

（二）多次出现个人信息违规出境等违法违规情形的；

（三）个人信息处理活动可能侵害众多个人权益的；

（四）发生个人信息安全事件，导致 100 万人以上个人信息或者 10 万人以上敏感个人信息泄露、篡改、丢失、毁损的；

（五）法律法规和有关主管部门规定的其他情形。

大型网络平台服务提供者应当配合第三方专业机构履行职责，为第三方专业机构开展工作提供必要保障，包括为第三方专业机构指定人员提供必要的访问大型网络平台网络数据设施、系统及操作日志记录权限等。

发现大型网络平台服务提供者无能力保障个人信息安全的，国家网信部门、国务院公安部门和有关主管部门可以要求大型网络平台服务提供者通过签订合同等方式将个

人信息存储在符合本规定要求的第三方数据中心。

第十八条 鼓励大型网络平台服务提供者应用国家网络身份认证公共服务、使用数据标签标识技术、通过个人信息保护认证等，提高个人信息保护水平。

第十九条 鼓励大型网络平台服务提供者开展个人信息保护相关技术、产品、服务创新，积极参与个人信息保护相关国际标准和规则制定，推动与其他国家、地区之间的个人信息保护规则、标准协调互认。

第二十条 任何组织和个人有权对大型网络平台服务提供者、第三方数据中心违反本规定的活动，向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当在 15 个工作日内依法处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当加强信息共享，协同开展相关工作。

第二十一条 网信部门、公安机关和有关主管部门发现大型网络平台服务提供者、第三方专业机构或者数据中心未履行个人信息保护责任的，依法追究责任；构成犯罪的，依法追究刑事责任。

第二十二条 国家网信部门、国务院公安部门和有关主管部门、第三方数据中心、第三方专业机构的工作人员应当对工作过程中知悉的个人隐私、个人信息、商业秘密、保密商务信息等依法予以保密，不得泄露或者非法向他人提供。

第二十三条 开展涉及国家秘密、工作秘密的个人信息处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

大型网络平台应当落实网络安全等级保护有关要求，属于关键信息基础设施的大型网络平台，还应当遵守国家关于关键信息基础设施安全的有关规定。

第二十四条 本规定自 X 年 X 月 X 日起施行。

《网络安全标识管理办法》（征求意见稿）

发文机关：国家互联网信息办公室

发布时间：2025.11.21

生效时间：待定

第一章 总则

第一条 为提升产品的网络安全能力，加强消费者权益保护，维护网络安全和公共利益，根据《中华人民共和国网络安全法》等法律法规，制定本办法。

第二条 本办法所称网络安全标识，是指能够反映产品本身网络安全能力水平的信息标识。

具有互联网联网功能的产品适用于本办法，具体产品实施目录管理。

第三条 网络安全标识管理工作坚持统筹发展和安全，产品生产者按照自愿原则参与。

鼓励产品生产者依据本办法提升产品网络安全能力，标注网络安全标识。

鼓励消费者优先选用标注网络安全标识的产品。

第四条 国家互联网信息办公室、工业和信息化部负责网络安全标识管理工作，分批制定公布《实施网络安全标识的产品目录》，明确每类产品的具体实施规则和依据的国家标准或技术文件，授权中国电子技术标准化研究院（以下简称“备案机构”）承担网络安全标识备案、信息发布、违规行为处置等工作。

第二章 标识实施

第五条 网络安全标识对应的网络安全能力由低到高依次为基础级、增强级、领先级，相应的标识等级分别用一星、二星、三星表示。基础级要求产品应当满足相关国家标准的基本安全要求，如不存在弱口令或通用默认口令、建立漏洞管理机制并动态修复

漏洞、保持软件更新等；增强级要求产品网络安全能力达到国内先进水平；领先级要求产品网络安全能力达到国际先进水平，同时还应通过渗透性测试方法，检测抵御高级别网络攻击的能力。

每类产品的标识等级具体安全要求，在实施规则中确定。安全要求应当和现行国家标准、国际标准做好衔接，充分借鉴吸收其它实施网络安全标识制度国家和地区的相关经验。

第六条 网络安全标识（英文名称为 China Cybersecurity Label）应当包括以下基本内容：

（一）产品生产者名称；

（二）产品规格型号；

（三）网络安全能力等级；

（四）网络安全标识有效期；

（五）检测实验室名称；

（六）依据的国家标准或技术文件编号；

（七）备案信息码，通过扫码可以获取检测报告、关键指标、产品生产者符合性声明等信息。

网络安全标识基本样式如下：

每类产品标识的具体样式应当在对应的实施规则中明确，可根据产品实际形态在上述基本样式基础上适当调整。

第七条 需要标注网络安全标识的产品，产品生产者应当依据实施规则相关要求开展网络安全能力检测，确定网络安全能力等级，并取得检测报告。

（一）需要标注一星级、二星级的产品，产品生产者可以利用自有检测实验室或者委托依法取得资质认定的第三方检测机构开展检测；

（二）需要标注三星级的产品，产品生产者在满足有关检测要求基础上，还应当委托符合条件的第三方检测机构开展渗透性测试。

第八条 备案机构建设网络安全标识备案管理平台，产品生产者备案网络安全标识通过平台线上办理。

备案时应当提交以下材料的电子版：

（一）网络安全标识备案表；

（二）网络安全能力等级检测报告；

（三）依据实施规则设计的本产品网络安全标识样式；

（四）产品生产者符合性声明；

（五）产品生产者营业执照；

（六）自有检测实验室的相关检测能力证明材料，或者第三方检测机构相关资质认定证书；

（七）由代理人提交备案材料的，还应当提交产品生产者的委托代理文件等。

产品生产者及代理人应当对上述材料的真实性、准确性、完整性负责。

第九条 备案机构应当自收到完整备案材料之日起 10 个工作日内，对材料的真实性、准确性、完整性进行形式审查，完成备案工作并公告产品相关备案信息。

备案完成后，产品生产者可以按照实施规则要求印制、使用和展示网络安全标识。

第十条 网络安全标识有效期在相关产品实施规则中明确。备案完成的产品，关键技术参数等发生变更可能影响产品网络安全能力的，或者标识超过有效期的，应当重新备案。

第十一条 任何组织和个人不得伪造、冒用网络安全标识或者利用网络安全标识进行虚假宣传。

第十二条 备案机构应当建立健全网络安全标识备案工作规范，客观、公正开展网络安全标识备案相关工作。

产品生产者自有检测实验室或者第三方检测机构应当严格按照有关标准开展检测，保证检测结果客观公正、真实准确，不得伪造检测结果或者出具虚假检测报告。

备案机构和检测机构不得泄露在工作中知悉的国家秘密、商业秘密。

第三章 监督管理

第十三条 国家互联网信息办公室、工业和信息化部负责组织对网络安全标识备案、使用情况进行监督检查，发现有违反本办法规定行为的，按照有关规定及时处理。

地方网信部门、通信管理局负责组织对本区域内网络安全标识使用进行监督检查，发现有违反本办法规定行为的，及时通知备案机构。

第十四条 发现以下情况，备案机构应当撤销备案并及时公告：

（一）备案材料弄虚作假的；

（二）网络安全标识与实际网络安全能力不相符的；

（三）使用的网络安全标识不符合有关样式、规格等标注规定的；

（四）产品生产者终止对备案产品开展技术支持服务的；

（五）其他应当撤销标识的违规行为。

第十五条 产品生产者伪造、冒用网络安全标识或者利用网络安全标识进行虚假宣传的，备案机构应当撤销相关产品的网络安全标识备案，对产品生产者违规行为予以公告，自公告之日起一年内不再受理其产品备案。

第十六条 产品生产者自有检测实验室或者第三方检测机构伪造检测结果或者出具虚假检测报告的，备案机构应当撤销相关产品的网络安全标识备案，对检测机构违规行为予以公告，自公告之日起一年内不再采信其检测结果。

第十七条 任何组织和个人发现违反本办法规定的行为，可以向地方网信部门、通信管理局举报。地方网信部门、通信管理局应当及时调查处理，并为举报人保密，调查过程中备案机构应当予以配合。

第十八条 网络安全能力检测过程中发现或者获知产品安全漏洞的，应当按照《网络产品安全漏洞管理规定》有关要求进行报告、修补和发布。

第四章 附则

第十九条 本办法所称网络安全能力，是指产品生产者通过采取必要技术和管理措施，使网络产品本身具备防范攻击、侵入、干扰、破坏和非法使用，保障产品稳定可靠运行和网络数据完整性、保密性、可用性的能力。

第二十条 网络关键设备和网络安全专用产品依据国家互联网信息办公室、工业和信息化部、公安部、财政部、国家认证认可监督管理委员会《关于调整网络安全专用产品安全管理有关事项的公告》（2023 年第 1 号）开展安全管理，不列入《实施网络安全标识的产品目录》。

第二十一条 本办法自 2026 年 月 日起施行。

附件 2：

实施网络安全标识的产品目录（第一批）

二、实务解读

1. 《大型网络平台个人信息保护规定（征）》解读一：负责人及工作机构的特殊合规要求

供稿人：黄春林（上海市汇业律师事务所）、袁姜涛（上海市汇业律师事务所）、钱静雯（上海市汇业律师事务所）

2025 年 11 月 22 日，国家网信办、公安部联合发布《大型网络平台个人信息保护规定（征求意见稿）》（以下简称《大平台规定》），作为《个人信息保护法》《数据安全法》等的落地细则和《网络数据安全管理条例》延伸补充，其核心要旨在于构建大平台的增强型合规体系，强化监管抓手，落实主体责任，筑牢风险围栏，树立大平台合规引领作用。

相较于一般个人信息处理者的基础合规要求，《大平台规定》强化了负责人及工作机构的设置要求，明确要求本地化存储，细化了个人信息权利行使及合规审计等规定，进一步夯实了大型平台的个人信息保护主体责任。

结合近期立法及监管实践，我们就大平台的负责人及工作机构的特殊合规要求解读如下，仅供参考。

一、大型网络平台的认定因素及机制

1. 认定的核心因素

延续《网络数据安全管理条例》的认定逻辑，《大平台规定》明确大型网络平台认定的三项核心因素：

- 用户规模的量化指标：注册用户 5000 万以上或月活跃用户 1000 万以上，此为

可量化的硬性门槛，也进一步倒逼企业坚持最小必要原则处理个人信息，及时删除不满足必要原则的数据。我们认为，实践中不宜将仅 Follow 企业的社交媒体的公众，仅浏览网页、小程序的游客，以及匿名购买的消费者等人群定义为“注册用户”；“月活跃用户”也应当根据行业特性，个案差异化认定。

- 业务重要性与复杂度的定性指标：提供重要网络服务或涵盖多类型业务，如同时运营社交、电商、支付等业务的综合平台，但并不以取得某个电信业务牌照（例如 ICP、EDI）为前提。
- 数据安全影响程度的风险指标：处理的数据一旦泄露、篡改等将对国家安全、经济运行、国计民生产生重大风险。

2. 各因素的关系

综合参考比对《未成年人网络保护条例》第二十条以及《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法（征求意见稿）》的立法技术，其对适用的网络平台就“用户数量”及“显著影响”进行了区分，并分别给出了判定标准。与之相对，我们认为《大平台规定》的前三项认定因素的适用逻辑则并非“满足其一”的“任一条件”模式，而是呈现“基础门槛+实质要件”的复合叠加判定模式，即需以用户规模指标为前提，同时结合业务属性与风险影响进行综合考量。

3. 认定机制

《大平台规定》确立了目录管理+动态更新的被动认定机制，而非企业自行主动判断，提高了企业合规建设的确定性。

值得注意的是，《大平台规定》中的合规要求虽仅针对大型网络平台，但其中的合规建设实践（例如负责人及工作机构职责划分），对一般个人信息处理者落地相关合规义务具有参考意义。

二、个人信息保护负责人的特殊合规要求

1. 任职要求

比照《网络数据安全管理条例》规定的重要数据处理者的网络数据安全负责人要求，《大平台规定》设定了个人信息保护负责人的三重任职要求：

- 身份资格限制：需具有中华人民共和国国籍，无境外永久居留权或长期居留许可，由境外 DPO 兼任的路径走不通了。
- 管理层级要求：必须由管理层成员担任，一般建议为副总裁及以上职级。
- 专业经验加码：需从事个人信息保护相关工作 5 年以上，这是一个相较于《网络数据安全管理条例》更加细化的要求。

相同的是，都可以兼任（例如数据安全负责人兼任），法条层面没有劳动合同的要求（但备案实践中可能需要）。此外，虽然这里没有强制要求对个人信息保护负责人开展背景审查，但我们仍然建议大平台开展背调并保留相关合规留痕。

2. 主要职责《大平台规定》赋予了三项核心权限与义务：

- 决策否决：参与个人信息处理事项决策时，对不合规事项拥有否决权。
- 领导管理：领导个人信息保护工作机构的日常工作，指导相关个保合规工作，落实相关监管要求，组织制定专门的未成年人个人信息处理规则。
- 监督行动：负责监督相关个人信息处理活动，并对安全风险及违法行为及时采取适当的处置措施。该条可能会受限于企业内部职能划分及资源情况，毕竟大多数企业的安全风险处置工作，是由安全或 IT 部门牵头。
- 直接报告：可直接向网信部门、主管部门等报告个人信息保护相关的情况。

3. 监管合规相较于针对负责人的监管合规要求，《大平台规定》进一步明确：

- 信息报送：需按照《关于开展个人信息保护负责人信息报送工作的公告》等规定依法报送负责人基本信息，此外，变更时需 20 个工作日内更新。
- 辅助监管：需配合有关部门开展个人信息保护监督检查；同时，发现安全风险和违法行为的，还应向国家网信部门和有关主管部门报告，涉嫌违法犯罪的应当向公安机关报案。该要求虽然法理上逻辑成立，但是可能会造成个保负责人的道德困境，反过来会造成对立，进而限制个保负责人了解、参与企业业务，甚至与个保负责人前述领导、决策权利形成直接利益冲突。

三、个人信息保护工作机构的特殊合规要求

1. 组织架构

《大平台规定》对工作机构的组织架构形成了基本框架：

- 链路定位明确：个人信息保护负责人由公司管理层担任，个人信息保护负责人直接领导工作机构日常工作，工作机构监督业务部门个人信息保护工作。此外，根据《网络数据安全管理条例》规定，企业还要成立主要由外部成员组成的个人信息保护监督机构。因此，形成了“负责人→工作机构→业务部门+外部监督机构”的组织框架。
- 专职化导向：鼓励设立专门的工作机构；即使依托现有部门，也需明确“专人专岗”负责个人信息保护，例如明确专人负责未成年人个人信息保护工作。

2. 主要职责

工作机构的职责在《大平台规定》中呈现“全链条+强监督”特征，具体的：

- 全链条负责机制：全面负责公司的个人信息保护相关的工作，包括制度建设、教育培训、风险管理、事件处置、投诉处理等工作。
- 平台“类监管”：借助工作机构夯实平台“类监管”责任，需明确平台内产品/服务提供者的个人信息处理规范，并对其履行义务情况进行监督。这就要求工作机构需要有实质的组织、人员及资源保障，确保该等形式+实质“类监管”责任的落地。
- 专项工作强制化：必须每年编制并发布个人信息保护社会责任报告。

3. 监管合规

《大平台规定》要求企业需向网信部门报送工作机构基本信息及保障履职措施等信息。

四、企业支持保障及个人职业规划

1. 企业支持

保障要求《大平台规定》将保障履职明确为企业的法定义务，具体的：

- 资源配置强制：企业需为负责人与工作机构提供必要的工作预算、人员编制、场所设备、保险等支持，且需在报备材料中列明具体保障措施，强化相关保障措施的有效性和落地性。
- 履职独立性：明确负责人享有否决权，以及可以直接向主管部门报告的任职保障。

2. 个人职业规划及准备

针对负责人与工作机构人员的要求，可梳理三类职业准备方向：

- 专业知识方面：建议加强个人信息保护、数据合规及网络安全方面的法律法规及专业知识学习，必要时可以考取第三方提供的认证或证书。
- 管理经验方面：建议加强参与个保相关项目的经验总结，确保相关工作及经验的留痕留档（例如任命书、项目合同、会议通知等），尤其注意挖掘 2020 年左右参与相关项目的支撑性材料，确保满足“五年”的量化指标。
- 其他方面：将潜在的任职限制纳入获取境外身份（包括港澳台）前的考量因素；购买相适应的商业保险；聘请专业顾问；锻炼个好身体……

为了进一步降低个人责任，我们建议个人信息保护负责人积极开展如下工作：

- 确保个人权责对等：公司提供与其法律义务和责任相对等的资源及保障，确保相关义务能够落地，确保相关责任有闭环。

- 尽快推动和完善公司个保合规建设：加快推进和完善个人信息保护影响评估、合规审计、权利响应、应急演练、教育培训等合规机制，确保合规留痕。

- 搭建更加广泛的合规管理平台：在工作机构的基础上，搭建业务、IT、人事及法务等相关部门负责人广泛参与的个人信息保护合规管理平台(例如委员会、协调小组等)，定期面向相关业务人员开展个人信息保护合规培训，有效传导合规压力，宣导合规意识，确保合规措施能够落地执行；等等。

2. 《大型网络平台个人信息保护规定（征）》解读二：数据本地化及其数据中心合规管理

供稿人：黄春林（上海市汇业律师事务所）、袁姜涛（上海市汇业律师事务所）、钱静雯（上海市汇业律师事务所）

2025 年 11 月 22 日，国家网信办、公安部联合发布《大型网络平台个人信息保护规定（征求意见稿）》（以下简称《大平台规定》），作为《个人信息保护法》《数据安全法》等的落地细则和《网络数据安全管理条例》延伸补充，其核心要旨在于构建大平台的增强型合规体系，强化监管抓手，落实主体责任，筑牢风险围栏，树立大平台合规引领作用。

作为《个人信息保护法》第四十条的落地细则，《大平台规定》不仅明确规定大平台数据本地化存储，同时也对大平台所使用的数据中心合规条件作出了更为具体的规范，进一步强化了责任链条。

结合近期立法及监管实践，我们就数据本地化及其数据中心合规管理解读如下，仅供参考。

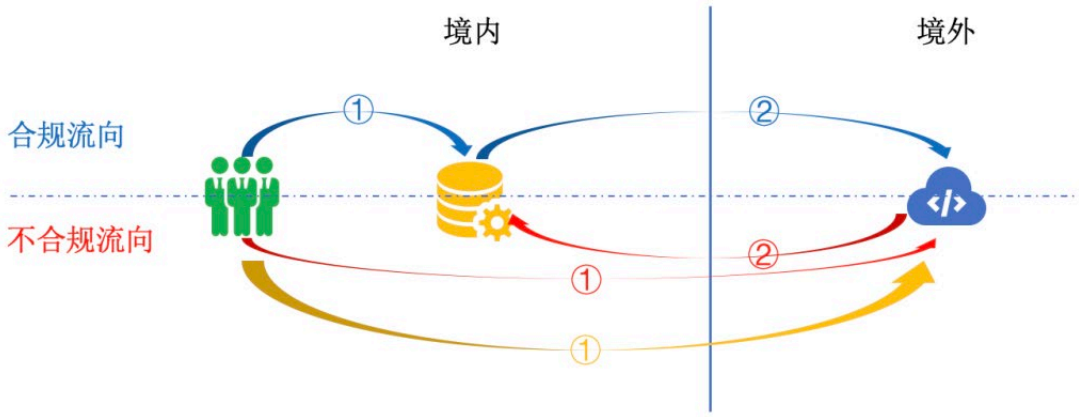
一、个人信息本地化存储要求

1. 受限个人信息范围

根据《大平台规定》第九条规定，本地化存储的规制数据范围为大平台在中华人民共和国境内运营过程中**收集和产生的所有个人信息，没有场景/系统（包括主要业务场景及支撑业务场景）、主体（不问主体身份是消费者/用户/患者/车主、员工、访客还是商业伙伴联系人，也不问主体的国籍）、敏感度（敏感个人信息及一般个人信息）及数量级（理论上哪怕 1 条）的任何例外**（不适用数据出境监管规定的豁免情形）。当然，这里仅限于个人信息，不含个人信息的非监管数据不受此限制。

2. 本地化存储要求

根据《大平台规定》第九条规定，**大平台应遵循“先内后外”的个人信息流向**，即大平台应当将境内运营过程中收集和产生的所有个人信息先存储在境内，再根据业务需要及合规路径向境外传输。需要特别说明的是，**这里只要求数据中心本地化，并不强制要求供应商国产化，即法律上不禁止大平台使用境外供应商在境内建立和运营的合规数据中心。**因此，以下几种个人信息流向的合规判断如下：



值得注意的是，近期部分地方网信办在 SCC 备案审查的时候，也会问询备案主体（非大平台）的数据本地化存储情况。

二、个人信息出境监管要求

数据本地化要求和数据出境监管，是两个相互独立又关联的制度，本地化并不绝对禁止数据出境。结合《个人信息保护法》《促进和规范数据跨境流动规定》《数据出境安全评估办法》等国家数据出境安全管理有关规定，就大平台个人信息出境监管相关的法律要求及近期政策实践，简要总结如下：

1. 个人信息出境必要性识别

尽管《大平台规定》未直接规定出境必要性审查的具体标准，根据近期政策实践，坚持“按需出境”原则，即数据出境的“必要性”应同时满足以下要件：(1) 出境场景必要，即拟出境场景是实现大平台业务功能的必要环节，不满足具体业务需求的场景不得出境；(2) 出境主体必要，严禁全量主体、全量数据出境；(3) 出境字段必要，即拟出境个人信息字段应控制在实现业务功能所需的最小范围，通常部分敏感字段可能不具有出境必要性。

2. 个人信息出境路径选择

个人信息出境主要通过三大类路径实现：一是根据拟出境的数据性质和数量阈值，依法开展出境安全评估或完成标准合同备案、个人信息保护认证；二是适用法律法规明确规定的豁免情形（但不豁免本地化）；三是如涉及向境外司法或执法机关提供境内存储的个人信息，应事前取得主管机关批准。

3. 个人信息出境安全保障

《大平台规定》《网络数据安全管理条例》等规定，大平台健全个人信息出境安全相关技术和管理措施，包括但不限于：建立数据出境安全管理制度，明确责任部门及岗位职责；加强平台内用户数据出境监管，协助国家采取措施，防范、处置平台内数据跨境安全风险和威胁；采取身份验证、数据加密、访问控制、日志留存等技术手段确保数据传输安全；等等。该等管理与技术措施应当做到全流程保障，覆盖个人信息出境前的风险评估、传输中的安全防护、出境后的持续监控等关键环节。

4. 个人信息出境安全事件处置

根据《大平台规定》《促进和规范数据跨境流动规定》等规定，大平台数据出境过程中发生或者可能发生数据安全事件的，应当采取补救措施，并根据《个人信息保护法》《国家网络安全事件报告管理办法》等要求，在规定时限内向国家网信部门、公安部门等主管部门报告事件情况，包括事件发生时间、影响范围、处置措施等。

三、合规数据中心的条件

1. 资质证照条件

资质证照要求方面，根据《中华人民共和国电信条例》《电信业务分类目录（2015年版）》等规定，仅经营性电信业务活动需要取得电信业务许可。具体而言：

在自建数据中心模式下，即大平台自建数据中心仅供其自身使用，不涉及对外出租向第三方提供数据中心服务的，则无需取得 IDC 资质，但自建数据中心仍应符合相关安全标准；

在租用数据中心模式下，即大平台使用第三方提供的数据中心服务的，则第三方向大平台提供数据中心服务即构成经营性电信业务活动，该等第三方需依法取得涵盖其业务范围及类别的 IDC 许可。

2. 资本条件

资本性质方面，自建和租用数据中心两种模式下，《大平台规定》均未对外资准入作出限制（目前，中国已经有部分外资成分数据中心），换句话说，**只要求数据中心本地化，并未要求供应商国产化。**

3. 地域条件

根据《大平台规定》第十条规定，数据中心必须设立在中华人民共和国境内，即自建与租用模式下的数据中心机房地理位置必须位于境内。**换句话说，即便是中国境内的云服务商（例如阿里云、华为云等）在海外建立的数据中心，也不符合《大平台规定》。**这对于大平台的数据中心容灾备份能力提出了挑战。

4. 负责人条件

根据《大平台规定》第十条规定，数据中心主要负责人需满足“双重条件”：(1) 具有中华人民共和国国籍；(2) 无境外永久居留权或者长期居留许可。实践中，第三

方数据中心在申请电信业务牌照时，就有法定代表人相关的身份限制。但是此处的“主要负责人”的具体范畴，有待监管实践进一步释明。

5. 合规管理能力条件

数据中心的合规管理能力包括但不限于：(1) 设置专业的合规管理团队和管理架构，负责数据中心的日常合规审查、风险防控等工作；(2) 健全个人信息保护组织管理制度和操作规程，确保个人信息存储、访问、使用等环节的安全性；(3) 制定数据安全事件应急预案，定期开展应急演练以应对潜在安全事件；(4) 配合大平台及监管部门的合规检查，提供必要的材料和技术支持。

6. 安全技术能力条件

数据中心的安全技术能力包括但不限于：(1) 依法取得必要的认证或备案，例如云安全审查、等保备案等；（2）其他技术安全细则，例如物理安全、数据安全、安全审计等，具体技术安全能力可进一步参考相关国家标准。

四、大平台对数据中心的合规管理要求

1. 资质审查

大平台应当对数据中心的资信及资质严格审查，审查内容应包括：(1) 数据中心的资质证照，包括营业执照、IDC 资质、系统等保备案证明等；(2) 核实数据中心的地域、负责人等条件是否符合《大平台规定》及要求；(3) 评估数据中心的合规管理能力和安全技术能力；等等。

2. 协议约束

若采用租用模式的，大平台应当与第三方数据中心签订书面协议，明确双方权利义务，协议内容应包括：(1) 由第三方数据中心承诺其提供的互联网数据中心服务符合法律法规要求，包括具备相应资质证照、安全技术能力等；(2) 约定具体合作内

容，如个人信息的存储地点、规模、种类等；(3) 明确第三方数据中心应当协助大平台履行个人信息保护义务，包括用户个人信息权利请求响应、信息公示及信息报送等；(4) 配合审计、检查要求，保障大平台的监督责任的实现；等。

法律关系上，第三方数据中心通常不允许“处理”租户（大平台）的数据（包括个人信息），因此大平台将个人信息存储在第三方数据中心的行为，是否属于《个人信息保护法》项下的委托处理，法理上值得商榷。当然，不同的 SaaS 服务商提供的服务实质不同，在《个人信息保护法》项下的法律地位各有差异。

3. 监督管理

根据《大平台规定》，数据中心应当接受大型网络平台服务提供者个人信息保护负责人、个人信息保护监督委员会等的监督。因此，若采用租用模式的，大平台需建立对数据中心的持续监督机制，可采用的方式包括：(1) 定期或风险事件触发时，对数据中心的合规情况进行检查、审计，包括资质有效性、安全措施落实情况等；(2) 要求数据中心定期提交合规审计报告，说明个人信息存储、安全保障等合规情况；等等。

4. 信息报送

根据《大平台规定》第十三条规定，无论采用的是自建模式还是租用模式，大平台均需向国家网信部门报送数据中心相关的信息，包括：(1) 管理团队和管理架构；(2) 内部个人信息保护管理制度、采取的安全措施；(3) 与第三方数据中心签署的合同文本（如涉及）等，并在相关信息发生变化的十个工作日内报送更正后的信息。参照大模型备案/登记机制，建议第三方数据中心常态化准备上述材料，以协助大平台租户履行信息报送合规责任。此外，**建议主管部门优化数据中心基本信息报送流程，由第三方数据中心自行向主管部门上传基本信息供所有租户共享，或者主管部门之间加强信息共享（工信部有第三方数据中心的基本信息），切实降低大平台租户分别提交的合规成本。**