

## 网络数据安全风险评估办法

**第一条** 为了规范网络数据安全风险评估活动，保障网络数据安全，促进网络数据依法合理有效利用，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》、《网络数据安全条例》等法律法规，制定本办法。

**第二条** 在中华人民共和国境内开展网络数据安全风险评估，应当遵守本办法。

本办法所称网络数据安全风险评估（以下简称风险评估），是指对网络数据和网络数据处理活动安全进行的风险识别、风险分析和风险评价等活动。

**第三条** 在国家数据安全工作协调机制指导下，国家网信部门会同国务院电信、公安等有关部门建立网络数据安全风险评估专项工作机制，指导、监督风险评估工作。

**第四条** 有关主管部门应当按照谁管业务、谁管业务数据、谁管数据安全的原则，定期组织开展本行业、本领域风险评估，根据工作需要对本行业、本领域处理重要数据的网络数据处理者（以下简称重要数据处理者）开展风险评估情况进行检查，并于每年1月底前将年度风险评估检查计划报送国家网信部门。国家网信部门通过国家数据安全工作协调机制将计划与国务院电信、公安、国家安全等有关部门共享并进行协调，避免不必要的检查和交叉重复检查。

有关主管部门开展检查不得向被检查的重要数据处理者收取费用。

**第五条** 重要数据处理者应当每年度开展风险评估。

重要数据安全状态发生重大变化可能对数据安全造成不利影响的，应当及时对发生变化及其影响的部分开展风险评估。

鼓励处理一般数据的网络数据处理者（以下简称一般数据处理者）至少每3年开展一次风险评估。

**第六条** 风险评估工作应当按照《中华人民共和国数据安全法》、《网络数据安全条例》有关要求，参照数据安全风险评估有关国家标准开展。有关主管部门对本行业、本领域风险评估工作另有规定的，从其规定。

**第七条** 网络数据处理者可以自行或者委托第三方评估机构（以下简称评估机构）开展风险评估。

网络数据处理者自行开展风险评估，应当指定专人负责。网络数据处理者委托评估机构开展风险评估，应当通过订立合同或者其他具有法律效力的文件等方式明确双方的权利、义务等。

**第八条** 鼓励相关评估机构通过认证。评估机构的认证按照《中华人民共和国认证认可条例》的有关规定执行。

**第九条** 在国家数据安全工作协调机制指导下，国家网信部门和国务院电信、公安等有关部门积极促进网络数据安全风险评估服务的发展，培育评估机构。

**第十条** 评估机构开展风险评估应当遵守法律法规，公正客观地作出风险判断，并对所出具的风险评估报告真实性、有效性、完整性负责。

**第十一条** 评估机构不得转委托其他机构开展风险评估。

**第十二条** 同一评估机构及其关联机构不得连续3次以上对同一网络数据处理者开展年度风险评估。

**第十三条** 评估机构在风险评估过程中发现网络数据处理活动存在重大数据安全风险的，应当及时通知网络数据处理者。

**第十四条** 评估机构及其工作人员应当对在风险评估过程中获得的数据、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，在风险评估结束后及时删除或者按照合同约定妥善处置相关信息。

**第十五条** 重要数据处理者开展年度风险评估，应当依法按照有关主管部门规定编制风险评估报告。有关主管部门对风险评估报告没有规定的，可以参照数据安全风险评估有关国家标准编制风险评估报告。风险评估报告至少保存3年。

一般数据处理者可以参照前款要求编制风险评估报告。

**第十六条** 重要数据处理者应当在年度风险评估完成后的20个工作日内按照有关主管部门要求向其报送风险评估报告。主管部门不明确的，向省级网信部门或者国家网信部门报送。

有关主管部门应当公开风险评估报告报送渠道和联系方式，及时接收重要数据处理者报送的风险评估报告，自收到风险评估报告之日起的10个工作日内将报告通报同级网信部门。国家网信部门汇总相关报告，并与国务院电信、公安、国家安全等有关部门共享。

省级以上网信部门、电信主管部门、公安机关、国家安全机关和其他有关部门可以对重要数据处理者的风险评估报告真实性、准确性进行检查核验，重要数据处理者应当配合开展检查核验。

**第十七条** 省级以上网信部门、电信主管部门、公安机关和其他有关部门在风险评估报告核验、监督检查等工作中发现网络数据处理者有以下情形之一的，可以要求其委托通过认证的评估机构开展风险评估：

- （一）网络数据处理活动存在较大安全风险，可能危害国家安全、公共利益的；
- （二）发生网络数据安全事件，导致重要数据或者大规模个人信息泄露、被窃取的；
- （三）有关部门规定的其他情形。

对同一网络数据安全事件或者风险，不得重复要求网络数据处理者委托评估机构开展风险评估。

**第十八条** 网络数据处理者按照有关部门要求委托评估机构开展风险评估的，应当履行下列义务：

- （一）为评估机构开展风险评估提供必要支持，包括为风险评估人员提供必要的访问网络数据设施、网络数据、系统及操作日志记录权限等；
- （二）在限定时间内完成风险评估，情况复杂的，报有关部门批准后可以适当延长；
- （三）在完成风险评估后将评估机构出具的风险评估报告报送有关部门，风险评估报告应当由评估机构主要负责人、风险评估负责人签字并加盖机构公章；
- （四）按照有关部门要求对风险评估中发现的问题进行整改，在整改完成后15个工作日内，向有关部门报送整改情况报告。

网络数据处理者不得以任何方式要求或者示意评估机构出具不实或者不当的风险评估报告。

**第十九条** 有关部门在组织开展风险评估中发现重要数据处理者的重要数据处理活动可能危害国家安全、公共利益的，应当依据职责责令重要数据处理者进行整改；对拒不整改或者未达到整改要求的重要数据处理者，可以采取要求其停止处理重要数据等措施。

**第二十条** 有关主管部门应当加强风险信息共享和协同处置，及时处置风险评估中发现的安全风险和问题，并按照有关规定及时报告。

**第二十一条** 任何组织、个人有权对风险评估中的违法活动向有关部门进行投诉、举报，收到投诉、举报的部门应当依法及时处理。

**第二十二条** 省级以上网信部门、电信主管部门、公安机关、国家安全机关或者其他有关部门发现网络数据处理者未按规定开展风险评估的，应当依据《中华人民共和国数据安全法》、《网络数据安全条例》等有关法律、行政法规予以处理。

发现评估机构违反本办法开展风险评估的，有关部门应当依法予以处理。

**第二十三条** 处理核心数据的网络数据处理者的风险评估，按照国家有关规定执行。

涉及重要数据加密等技术措施的，应当按照国家密码相关法律、行政法规要求开展商用密码应用安全性评估。

**第二十四条** 开展涉及国家秘密、工作秘密的风险评估活动，按照《中华人民共和国保守国家秘密法》等法律、行政法规及国家保密规定执行。

**第二十五条** 本办法自2026年8月20日起施行。