**个人信息和重要数据出境安全评估办法**

**（征求意见稿）**

**第一条** 为保障个人信息和重要数据安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法利益，根据《中华人民共和国国家安全法》《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** 网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。

**第三条** 数据出境安全评估应遵循公正、客观、有效的原则，保障个人信息和重要数据安全，促进网络信息依法有序自由流动。

**第四条** 个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。

**第五条** 国家网信部门统筹协调数据出境安全评估工作，指导行业主管或监管部门组织开展数据出境安全评估。

**第六条** 行业主管或监管部门负责本行业数据出境安全评估工作，定期组织开展本行业数据出境安全检查。

**第七条** 网络运营者应在数据出境前，自行组织对数据出境进行安全评估，并对评估结果负责。

**第八条** 数据出境安全评估应重点评估以下内容：

    （一）数据出境的必要性；

    （二）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等；

    （三）涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；

    （四）数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；

    （五）数据出境及再转移后被泄露、毁损、篡改、滥用等风险；

    （六）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；

    （七）其他需要评估的重要事项。

**第九条** 出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估：

    （一）含有或累计含有50万人以上的个人信息；

    （二）数据量超过1000GB；

    （三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；

    （四）包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；

    （五）关键信息基础设施运营者向境外提供个人信息和重要数据；

    （六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。

    行业主管或监管部门不明确的，由国家网信部门组织评估。

**第十条** 行业主管或监管部门组织的安全评估，应当于六十个工作日内完成，及时向网络运营者反馈安全评估情况，并报国家网信部门。

**第十一条** 存在以下情况之一的，数据不得出境：

    （一）个人信息出境未经个人信息主体同意，或可能侵害个人利益；

    （二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；

    （三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

**第十二条** 网络运营者应根据业务发展和网络运营情况，每年对数据出境至少进行一次安全评估，及时将评估情况报行业主管或监管部门。

    当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，应及时重新进行安全评估。

**第十三条** 对违反相关法律法规和本办法向境外提供数据的行为，任何个人和组织有权向国家网信部门、公安部门等有关部门举报。

**第十四条** 违反本办法规定的，依照有关法律法规进行处罚。

**第十五条** 我国政府与其他国家、地区签署的关于数据出境的协议，按照协议的规定执行。

    涉及国家秘密信息的按照相关规定执行。

**第十六条** 其他个人和组织在中华人民共和国境内收集和产生的个人信息和重要数据出境的安全评估工作参照本办法执行。

**第十七条** 本办法下列用语的含义：

    网络运营者，是指网络的所有者、管理者和网络服务提供者。

    数据出境，是指网络运营者将在中华人民共和国境内运营中收集和产生的个人信息和重要数据，提供给位于境外的机构、组织、个人。

    个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

    重要数据，是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。

**第十八条** 本办法自2017年 月 日起实施。