数据出境安全评估办法

2022年07月07日 16:30 来源：中国网信网 【打印】【纠错】

国家互联网信息办公室令

第11号

《数据出境安全评估办法》已经2022年5月19日国家互联网信息办公室2022年第10次室务会议审议通过，现予公布，自2022年9月1日起施行。

国家互联网信息办公室主任 庄荣文

2022年7月7日

数据出境安全评估办法

第一条 为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，制定本办法。

第二条 数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息的安全评估，适用本办法。法律、行政法规另有规定的，依照其规定。

第三条 数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障数据依法有序自由流动。

第四条 数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：

（一）数据处理者向境外提供重要数据；

（二）关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息；

（三）自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息；

（四）国家网信部门规定的其他需要申报数据出境安全评估的情形。

第五条 数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项：

（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

（二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务；

（六）其他可能影响数据出境安全的事项。

第六条 申报数据出境安全评估，应当提交以下材料：

（一）申报书；

（二）数据出境风险自评估报告；

（三）数据处理者与境外接收方拟订立的法律文件；

（四）安全评估工作需要的其他材料。

第七条 省级网信部门应当自收到申报材料之日起5个工作日内完成完备性查验。申报材料齐全的，将申报材料报送国家网信部门；申报材料不齐全的，应当退回数据处理者并一次性告知需要补充的材料。

国家网信部门应当自收到申报材料之日起7个工作日内，确定是否受理并书面通知数据处理者。

第八条 数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项：

（一）数据出境的目的、范围、方式等的合法性、正当性、必要性；

（二）境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；

（三）出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；

（四）数据安全和个人信息权益是否能够得到充分有效保障；

（五）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；

（六）遵守中国法律、行政法规、部门规章情况；

（七）国家网信部门认为需要评估的其他事项。

第九条 数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容：

（一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；

（二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；

（三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；

（四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；

（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；

（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

第十条 国家网信部门受理申报后，根据申报情况组织国务院有关部门、省级网信部门、专门机构等进行安全评估。

第十一条 安全评估过程中，发现数据处理者提交的申报材料不符合要求的，国家网信部门可以要求其补充或者更正。数据处理者无正当理由不补充或者更正的，国家网信部门可以终止安全评估。

数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。

第十二条 国家网信部门应当自向数据处理者发出书面受理通知书之日起45个工作日内完成数据出境安全评估；情况复杂或者需要补充、更正材料的，可以适当延长并告知数据处理者预计延长的时间。

评估结果应当书面通知数据处理者。

第十三条 数据处理者对评估结果有异议的，可以在收到评估结果15个工作日内向国家网信部门申请复评，复评结果为最终结论。

第十四条 通过数据出境安全评估的结果有效期为2年，自评估结果出具之日起计算。在有效期内出现以下情形之一的，数据处理者应当重新申报评估：

（一）向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；

（二）境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；

（三）出现影响出境数据安全的其他情形。

有效期届满，需要继续开展数据出境活动的，数据处理者应当在有效期届满60个工作日前重新申报评估。

第十五条 参与安全评估工作的相关机构和人员对在履行职责中知悉的国家秘密、个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供、非法使用。

第十六条 任何组织和个人发现数据处理者违反本办法向境外提供数据的，可以向省级以上网信部门举报。

第十七条 国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。

第十八条 违反本办法规定的，依据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规处理；构成犯罪的，依法追究刑事责任。

第十九条 本办法所称重要数据，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

第二十条 本办法自2022年9月1日起施行。本办法施行前已经开展的数据出境活动，不符合本办法规定的，应当自本办法施行之日起6个月内完成整改。