



数据合规专题

第九期

数据存储的合规性要求（上）

（2025 年 4 月）

作为数据处理过程中的重要组成部分，数据的合规存储不仅关系到数据处理器能否继续收集使用数据，更与数据权利主体的切身利益密切相关。在收集数据后，数据处理器应严格履行数据存储的期限、地点及安全等方面的法定义务及与数据权利主体之间的约定义务，避免数据泄露事件的发生，维护数据权利主体的合法权益。

《数据的合规存储》专题分为上、下两篇，本篇旨在阐释数据的存储期限及存储位置，数据存储安全事宜将在下篇中具体阐述。

一、存储期限

现行法律法规根据数据类型及行业管理要求，规定了不同数据的存储期限。数据处理器可以在满足法定要求的前提下与数据权利主体就存储期限作出进一步约定并严格按照约定执行。

1、数据存储期限的一般规定

（1）**个人信息存储期限**。根据《中华人民共和国个人信息保护法》的规定，除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。若个人信息处理者在法定情形下，包括处理敏感个人信息、利用个人信息进行自动化决策、向境外



提供个人信息、委托处理个人信息、向其他个人信息处理者提供个人信息或公开个人信息等，事先进行个人信息保护影响评估的，个人信息保护影响评估报告和处理情况记录应当至少保存三年。

（2）**网络日志存储期限**。根据《中华人民共和国网络安全法》的规定，网络运营者应当采取监测、记录网络运行状态、网络安全事件的技术措施，如：入侵检测及防御系统、异常行为分析、追踪及溯源等，并按照规定留存相关的网络日志不少于六个月。

2、各行业关于数据存储期限的特殊要求

基于各行业的管理要求，法律法规对不同行业所涉数据的存储期限进行了差异化规定。例如：

（1）《征信业务管理办法》规定，征信机构采集的个人不良信息的保存期限，为自不良行为或者事件终止之日起5年，保存期限届满后应当删除，作为样本数据的，应当进行匿名化处理。

（2）《网络交易监督管理办法》规定，网络交易平台经营者对平台内经营者身份信息的保存时间自其退出平台之日起不少于三年；对商品或者服务信息，支付记录、物流快递、退换货以及售后等交易信息的保存时间自交易完成之日起不少于三年。网络直播服务提供者对网络交易活动的直播视频保存时间自直播结束之日起不少于三年。

（3）《银行保险机构数据安全管理办法》规定，核心数据操作日志及其备份数据保存时间不低于三年，重要数据、敏感数据操作日志及其备份数据保存时间不低于一年，如涉及委托处理、共同处理的数据操作日志及其备份数据保存时间不低于三年。



上述核心数据，是指对领域、群体、区域具有较高覆盖度或者达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或者共享，可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益；重要数据，是指特定领域、特定群体、特定区域或者达到一定精度和规模的数据，一旦被泄露或者篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全；敏感数据，是指一旦被泄露或者篡改、损毁，对经济运行、社会稳定、公共利益有一定影响，或者对组织自身或者公民个体造成重要影响的数据。

（4）《网络预约出租汽车经营服务管理暂行办法》规定，网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于2年，除法律法规另有规定外，上述信息 and 数据不得外流。

（5）《缺陷汽车产品召回管理条例》规定，生产者应当建立并保存汽车产品设计、制造、标识、检验等方面的信息记录以及汽车产品初次销售的车主信息记录，保存期不得少于10年。

因此，数据处理者应当时刻关注并遵守所处行业对数据存储期限的特定要求及规定。

二、存储位置

当前，我国法律法规仅对特定数据的存储位置作出了特别规定。在无特别规定的情况下，数据处理者可根据数据权利主体的授权或与数据权利主体之间的具体约定确定数据的存储位置。现就部分常见数



据存储的特殊规定总结如下：

1、个人信息

根据《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》等法律法规规定，国家机关处理的个人信息，以及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在中华人民共和国境内收集和产生的个人信息，应当存储在境内，确需向境外提供的，除法律法规另有规定外，应当进行安全评估。

上述关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。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，包括处理100万人以上个人信息的数据处理者，以及自上年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。

2、重要数据

根据《中华人民共和国网络安全法》的规定，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，如：涉及国家地理信息、经济统计数据、航空调度系统数据、重大传染病监测数据、核心知识产权数据等，应当在境内存储。因业务需要，确需向境外提供的，除法律法规另有规定外，应当进行安全评估。

3、其他特殊规定



基于上述规定,各行业在自身管理规定中也对此予以明确。例如:

(1)《征信业务管理办法》明确,征信机构在中华人民共和国境内开展征信业务及其相关活动,采集的企业信用信息和个人信用信息应当存储在中华人民共和国境内。征信机构向境外提供个人信用信息,应当符合法律法规的规定;征信机构向境外信息使用者提供企业信用信息查询产品和服务,应当对信息使用者的身份、信用信息用途进行必要的审查,确保信用信息用于跨境贸易、投融资等合理用途,不得危害国家安全。(2)《汽车数据安全若干规定(试行)》规定,重要数据应当依法在境内存储,因业务需要确需向境外提供的,应当通过国家网信部门会同国务院有关部门组织的安全评估。未列入重要数据的涉及个人信息数据的出境安全管理,适用法律、行政法规的有关规定。(3)《医疗卫生机构网络安全管理办法》规定,各医疗卫生机构应加强数据收集、存储、传输、处理、使用、交换、销毁全生命周期安全管理工作,数据全生命周期活动应在境内开展,因业务确需向境外提供的,应当按照相关法律法规及有关要求进行安全评估或审核,针对影响或者可能影响国家安全的数据处理活动需提交国家安全审查,防止数据安全事件发生。

因此,若数据处理者处理的数据涉及个人信息及重要数据的,应当在中国境内存储数据,确需向境外提供的,应当按照法律法规规定完成安全评估等工作。

北京道商律师事务所



2025 年 4 月【 】日