



数据合规专题

第十六期

数据的删除及销毁

(2025 年 11 月)

实践中，数据处理者往往重点关注数据的收集与使用，却时常忽视了数据的删除与销毁。作为数据生命周期管理的最后一环，若在该环节出现数据泄露或其他数据安全事故，将导致数据合规管理功亏一篑。因此，数据处理者应当依法采取必要举措保障数据安全，确保数据处理全流程的合法合规。

一、数据的删除

数据删除，是指对存储空间或介质中的数据进行技术处理，使数据不可被读取、访问或恢复的活动或过程。数据删除的法定情形主要见于《中华人民共和国个人信息保护法》(下称“《个人信息保护法》”)以及部分行业主管部门颁布的相应规范或指南中。

个人信息的删除是指在实现日常业务功能所涉及的系统中去除个人信息，使其保持不可被检索、访问的状态。根据《个人信息保护法》第四十七条规定，个人信息处理者应当删除数据的情形包括但不限于：处理目的已实现、无法实现或者为实现处理目的不再必要；个人信息处理者停止提供产品或者服务，或者保存期限已届满；个人撤回同意；个人信息处理者违反法律、行政法规或者违反约定处理个人



信息；法律、行政法规规定的其他情形。若法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

部分行业主管部门亦对本行业内相关数据的删除情形作出规定。例如，《中国人民银行业务领域数据安全管理办法》规定，中国人民银行业务领域数据（下称“业务数据”）指中国人民银行业务领域内产生和收集的不涉及国家秘密的网络数据。数据处理者应当依照法律、行政法规和中国人民银行相关规定，主动删除处理目的已实现、处理目的无法实现、为实现处理目的不再必要或者约定保存期限已届满等情形的业务数据。删除业务数据从技术上难以实现的，数据处理者应当停止除存储和采取必要的安全保护措施之外的业务数据处理活动，并每年至少实施一次审查，确认相关业务数据不可被使用。

对于数据删除，数据处理者须采取适当方式确保删除的有效性 & 数据的安全性。根据《数据安全技术 数据安全风险评估方法》（GB/T 45577-2025，下称“《数据安全风险评估方法》”）的规定，数据删除管理的重点评估事项主要包括：数据删除流程和审批机制的建设落实情况；数据删除安全策略和操作规程；是否按照法律法规、合同约定、隐私政策等及时删除数据；委托第三方进行数据处理的，是否在委托结束后监督第三方删除或返还数据；数据删除有效性、彻底性验证情况，以及可能存在的多副本同步删除情况；是否明确数据存储期限，并于存储期限到期后按期删除数据，明确不可删除数据的类型及原因；缓存数据、到期备份数据的删除情况；个人信息处理者是否依法履行



删除义务等。

二、数据的销毁

数据销毁是指使用数据覆盖、介质消磁、硬件破坏等技术手段，清除存储介质上部分或全部数据的操作。相较于数据删除，数据销毁在数据清除效果上更加强调删除的彻底性及数据的不可恢复性。

结合《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）的规定，数据销毁安全包括数据销毁处置及存储媒体销毁处置两个方面。数据销毁处置为通过建立针对数据的删除、净化机制，实现对数据的有效销毁，防止因对存储媒体中的数据进行恢复而导致的数据泄漏风险。存储媒体销毁处置为通过建立对存储媒体安全销毁的规程和技术手段，防止因存储媒体丢失、被窃或未授权的访问而导致存储媒体中的数据泄漏的安全风险。

对于数据销毁，数据处理者可参考《数据安全风险评估方法》及《网络安全技术 存储介质数据恢复服务安全规范》（GB/T 31500-2024）的规定执行。其要求包括但不限于：数据处理者在数据交付完成后应根据协议约定及时销毁数据恢复结果及操作过程中产生的所有相关数据信息，并在销毁审批后以不可逆方式销毁数据及其副本内容；重要数据级别以上的数据，应在销毁审批后实施现场销毁，并在必要情况下实施数据恢复验证；数据处理者应建立数据销毁及存储介质销毁的审批机制和管理制度，明确销毁对象、销毁策略和操作规程，按照数据分类分级明确不同级别数据的适用措施，并建立数据销毁审批机制记录数据销毁操作时间、操作人、操作方式，确认介质



销毁措施的有效性等。

综上，在现行法律框架下，仅《个人信息保护法》对个人信息的删除作出了明确统一的规定，对于其他类型的数据应否删除或销毁、应采取销毁还是删除的方式需根据主管部门发布的相关规定确定。除此之外，在数据流转或处理的过程中，数据提供者、数据处理者也可根据实际需要约定数据删除或销毁的情形，并可参考上述《数据安全风险评估方法》及《网络安全技术 存储介质数据恢复服务安全规范》的要求确定数据删除或销毁的标准，以确保数据的完整性、真实性及安全性。

北京道商律师事务所

2025 年 11 月