

数据泄露事件预防与应对

作者：段志超 | 胡敏喆

近年来，数据安全事件频发。为提升数据安全保护能力、降低数据安全事件造成的损失和危害，《网络安全法》《数据安全法》和《个人信息保护法》（下称“三部立法”）均要求企业采取安全保护措施，制定和实施网络安全事件应急预案。2023年12月8日，国家互联网信息办公室（下称“网信办”）发布《网络安全事件报告管理办法（征求意见稿）》（下称“《征求意见稿》”），拟对网络安全事件的监管报告要求做出统一规范。本文将根据这些法律法规的要求，结合近期监管动态和实务经验，从事前预防、事发应对两个方面介绍数据安全事件处置的合规要点。

一、事前预防

三部立法分别规定了企业应采取的安全保护措施，包括但不限于数据加密、防范计算机病毒和网络攻击及侵入、留存网络日志等。这些措施不仅能提升企业的数据安全保护能力，也有助于企业及时发现和监测安全事件。

为预防数据泄露事件，三部立法要求企业制定应急预案、加强风险监测。其中，制定应急预案是企业及时处置数据安全事件的必要前提。跨国集团需在普遍适用于全球的管理制度基础上，制定符合中国法要求的“本地化”方案。此外，为确保应急预案真正落地，企业还需定期开展应急响应演练，帮助各部门员工熟悉响应流程，并根据发现的问题及时调整预案。

二、事发应对

（一）及时补救

企业技术人员可参考《信息安全技术网络安全事件分类分级指南》《信息安全技术信息安全应急响应计划规范》等国家标准，在应急预案中制定针对不同级别和类型数据安全事件的处置措施和流程，并在事发后及时启动预案并采取补救措施。

（二）通知个人

根据《个人信息保护法》第五十七条第一款规定，若遭到泄露、篡改、丢失的数据涉及个人信息，企业应当向个人告知涉及的个人信息种类、原因和危害、企业已经采取的措施和个人可以采取的减轻危害的措施以及企业的联系方式。

《信息安全技术个人信息安全规范》（下称“《规范》”）建议企业通过邮件、信函、电话、推送通知等方式逐一告知，或采取合理、有效的方式发布警示信息。尽管《个人信息保护法》还规定了豁免通知的情形，但如何定义和评估“有效避免危害”缺乏明确的认定标准，企业应持审慎态度并遵从监管机关的要求。

（三）上报监管

1. 报告门槛

现行法律法规并未设置明确的标准，理论上任何数据安全事件均应向监管部门报告。不过，《国家网络安全事件应急预案》等相关规定则要求上报“对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响”的安全事件。企业可以在个案中结合数据类型、受影响的范围和人数、经济损失等综合评估是否达到这一标准。

2. 报告对象

三部立法对此规定较为笼统。实践中，网信部门是主要负责接收企业报告的监管机构，工信部、应急管理部、行业主管部门也在其职责范围内接收企业的报告。当数据安全事件涉及刑事犯罪时，企业还需向公安机关报告。由于不同监管机构之间的协调机制暂不明晰，建议企业在报告时主动咨询可能涉及的部门，并按照监管指示履行报告义务。

3. 报告内容

除向个人告知的事件基本信息外，《征求意见稿》第五条还进一步要求企业提供涉事设施、系统、平台的情况，事态发展趋势及可能进一步造成的影响和危害、进一步调查分析所需的线索、请求支援事项和事件现场的保护情况等。在报告内容的呈现形式方面，《征求意见稿》及一些地方法规要求企业根据制式的报告表提供相关内容。

4. 报告时限

现行法律要求企业在事件发生后“及时”或“立即”履行报告义务。《征求意见稿》要求企业在小时内报告较大、重大或特别重大的网络安全事件。如果前述法规正式生效，企业的准备时间将十分有限。相关部门和人员需充分了解本企业的应急预案，快速收集信息，并在规定时限内与监管机关保持密切沟通。

（四）反思与整改

为避免类似事件再次发生，《规范》第 10.1 条建议企业整理留存事件记录文件，总结安全事件防范及应急处置工作中的经验教训，并据此开展必要的整改工作，进一步完善数据安全保护措施。

三、结语

企业未履行数据安全保护义务、违反数据安全事件处置合规要求，最高面临 5,000 万元或上一年度营业额 5% 的罚款，直接负责的主管人员和其他直接责任人员也可能面临高达 100 万的罚款。实践中，企业遭遇数据安全事件后，因未履行数据保护义务而受到处罚的案件殷鉴不远，这无疑为企业的个人信息保护和数据安全事件应急处置敲响了警钟。建议企业在开展日常业务时，严格落实数据保护要求，做好安全事件的预防和准备工作，并在事发后根据适用法律的要求履行合规义务。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123

Email: kevin.duan@hankunlaw.com