君合专题研究报告

2023 年 2 月 24 日

跨境数据监管合规系列（一）：数据泄露事件中的跨境监管和个人责任

数据泄露事件泛指绕过基本安全机制导致敏感或关键数据被盗或暴露给未授权方的安全事件。这些事件可能由故意引发，例如遭受勒索攻击、离职或内部人员泄密，也可能因疏忽导致，例如存有数据的电脑或手机遗失。近年发生的数据泄露事件显示，不同规模或行业的企业均无法完全避免网络攻击或出现数据泄露，掌握大量个人信息的企业尤其可能因数据泄露产生经济和商誉损失。

因业务和信息设施架构的全球性，引发较高舆论关注的数据泄露事件往往与跨国企业相关，并常常涉及多个法域的监管执法。因此，数据泄露事件的处置不是一个简单的问题，不可避免地围绕**网络安全、跨境监管要求、数据流动、个人隐私和安全**等多项因素的潜在权衡展开。对于跨国企业来说，数据泄露事件的处置已是一项日趋复杂的挑战。

结合我们实务中的经验，以及中国网络安全和数据保护监管特点，本文将着重讨论**数据泄露事件处理的重点，“本地化”方案的必要性，高管等个人责任风险，以及合规挑战和专业团队支持**。

一、数据泄露事件处置的重点

不同国家或地区的立法对数据泄露事件的监管理念整体以个人信息和网络数据安全的保护为原则，但在具体的处置要求上则存在差异。这要求企业一方面需要在面对跨国监管要求时，保持各地区之间的信息同步，确保总部与各地区的经营主体步调一致；另一方面，企业也需要针对不同法域的规定，采取恰当的处置策略与方案。

以上报要求为例，我国《个人信息保护法》规定，在发生或可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知监管部门。[1] 该等规定并未设置豁免或例外情形，对于涉及在中国处理个人信息的企业来说，意味着一旦遭遇个人信息泄露事件，即需尽快考虑上报准备的情况。而欧洲《数据通用保护条例》（General Data Protection Regulation）规定，在企业意识到数据泄露事件发生时，应在 72 小时内进行报告，但数据泄露不会对个人权利和自由造成风险的情况除外。[2] 新加坡《个人信息保护法案》（Personal Data Protection Act）规定，如果数据泄露导致个人造成重大损害，或影响 500 人以上时，企业须立刻通知个人资料保护委员会和受影响的个人。[3]

对于跨国企业来说，当数据泄露事件涉及多个国家或地区时，企业往往需在发现数据泄露事件或

[1] 《个人信息保护法》第 57 条
[2] 欧洲《数据通用保护条例》第 33 条, https://gdpr-info.eu/art-33-gdpr/
[3] 新加坡《个人数据保护法案》2021 年修正案 https://sso.agc.gov.sg/SL-Supp/S64-2021/Published/20210129?DocDate=20210129

迹象后的很短时间内（甚至可能是数小时内），迅速评估并决定处置方案。而实际处置方案并没有完美的参考答案，且需要具有丰富经验、可信赖的跨国法律和技术服务团队鼎力合作，并能够由企业和各方专业人士尽快制定工作方案。跨国企业在制定处置方案与行动计划时，一般需要考虑以下问题：

（1）**事件严重程度**：数据泄露事件的影响范围和严重程度，例如受影响的系统和服务器范围，被访问的数据是否包括员工或客户个人隐私，或包含公司重要商业信息，该等数据是否确实被非法下载或导出，公司受影响的数据是否在黑产舆情、暗网情报、代码托管平台（如 GitHub、Gitee）等渠道出现，是否可能出现进一步的刑事犯罪风险（如个人信息主体遭受诈骗）。

（2）**采取补救措施**：公司应采取哪些补救及处置措施，例如能否在不同区域适用统一的处理方案，是否需要尽快向受影响的个人主体提供补偿，不恰当的通知或补救措施是否会进一步引发个人信息主体（如员工、消费者）的不满。

（3）**重点司法区域**：数据泄露事件涉及哪些司法管辖区，并将触发何等合规义务，例如当地法规对违规行为的定义，是否要求短时间内向监管部门报告，对于报告的内容和形式要求，上报或通知义务有无例外或豁免情形。

（4）**特殊情况考量**：基于对事件所涉主要司法区域的了解，需要针对特定司法区域进行特殊考虑，例如中国数据出境监管和本地化要求考量下的技术供应商的选择（如能否将涉及国内收集数据的镜像硬盘直接传递出境或将其数据直接存储于位于境外的服务器中）；美国“律师特权保护”在数据泄露事件中的运用；以及对于跨司法区域、复杂的数据泄露事件中其他法律风险的评估和准备（如集体诉讼）。

二、跨境监管框架下的“本地化”方案

以上考虑因素并非完整列举，比较合理的设计和实施处置方案的基本思路是——在企业全球化数据和网络安全管理框架内，围绕本地法规监管要求，通过“本地化”的措施和安排，尽可能降低数据泄露事件对企业的负面影响。除本地法规要求外，跨境数据泄露事件处置中另两项比较重要的“本地化”因素则包括：

（1） “本地化”的团队支持

根据我们的经验，跨境数据泄露事件的响应往往遵循如下流程：企业通过内部或外部途径发现数据泄露迹象→IT 部门上报事件至管理层，并同步法务、公共关系等部门→公司指定事项响应负责人（或团队）主导事件的调查和处理→必要时，聘请外部法律、技术团队（如 forensic investigation）协助调查开展（在大规模的跨境泄露事件中尤其常见）→对事件的具体情况和监管义务履行等进行评估、决策→事后复盘并加强安全机制和预防措施。对于跨国企业来说，前述流程的设置一般遵循企业既定的应急预案，对于数据和信息安全管理制度比较完善的企业来说，甚至已经准备好了详细的执行要求和场景化提示，以便在数据泄露发生时，能够快速启动应急预案，避免层层报批带来的时间流失以及事件影响的扩大。

在上述常规流程的开展中，“本地化”的团队支持是不可忽略的因素。“本地”的团队不仅指本地的 IT、法务、公共关系等部门的直接参与，也包括聘请“本地化”的外部法律、技术和法证调查或技术服务团队等。“本地化”团队的直接介入甚至承担主导角色（当数据泄露事件主要涉及当地时）一般来说可以取得更好的事件处置效果，主要由于本地化的团队（如律师）对当地监管要求以及执法情况更为熟悉，而本地的 IT 技术团队对企业在当地的系统或服务器情况、数据资料管理情况更为了

解，可以显著加快调查和分析进展。

（2）“本地化”的措施应用及中国法合规考量

除了“本地化”的团队支持，在数据泄露事件的处置中，因地制宜的“本地化”补救措施也需纳入考量。由于不同国家或地区对数据泄露事件补救的措施要求和操作惯例存在差异，直接套用境外总部安排的补救措施可能出现无法落地或适得其反的效果。例如，在大规模数据泄露事件中，美国或英国的部分企业常常主动为受影响的个人提供一段时间（如 6 个月）的信用监视（credit monitoring）服务，以提醒受影响的个人注意其信用报告或分数的变化。这类措施一定程度上有助于减轻企业因数据泄露可能面临的处罚。然而由于信用机构运营和信用评价监管方式的差异，多数国家（如中国、欧盟）并无类似的服务，故跨国企业的全球化补救方案中如有此类措施，则应注意调整。

比较普遍的补救措施诸如修复漏洞、封锁环境、限制访问，通常综合费用成本、实施效率和预期效果考虑，技术方面整体以公司内部 IT 和外部技术团队的意见为准。对于法律团队来说，更重要的则是提供法律合规和策略指导，包括：（1）分析确定监管报告的必要性；（2）确定内外部通信和告知的口径；（3）对于涉及企业客户（尤其是个人用户或消费者的），与销售或服务部门协同制定客户支持和管理方案。在拟定前述措施前，则需要协同 IT 和技术团队尽快确定事件的原因、性质和影响范围。

需要特别注意的是，当涉及在中国处理的数据发生泄露事件时，需要考虑中国网络安全和数据安全特殊监管要求，包括**数据出境的监管要求，网络安全报告义务，以及当涉及敏感行业、敏感信息时的国家安全考量**。对于跨国企业来说，一旦涉及在中国境内收集或处理的数据发生网络安全事件，不应仅考虑美欧等司法区域的应对措施，还需考虑中国网络安全合规的要求。中国律师的参与和协调，将是确保事件处理本身符合中国法律要求，避免引发其他合规问题的必要措施。

三、潜在的高管个人责任

目前大部分数据泄露事件最终都由企业承担法律责任。但是若高管不当行为是泄露事件发生的主要原因之一时，则高管仍有承担个人责任的风险。例如，中国的法律对于个人责任有着较为普遍的适用。《个人信息保护法》、《数据安全法》和《网络安全法》都规定了“双罚制”，对于未能履行网络或数据安全保护义务的企业，同时对企业、直接负责的主管人员和其他直接责任人员施以行政处罚。如果数据安全事件的情节严重，相关责任人员可能会面临上至一百万元的罚款，也可能面临一定期限的从业限制。

在欧美等地，高管的个人责任也逐渐被引入到了监管部门的执法行动中。2023 年初，美国联邦贸易委员会（FTC）针对一家电商平台及其首席执行官泄露 250 万名消费者个人信息的案件中，FTC 除了追究公司责任外，对于首席执行官个人，FTC 要求其在 10 年内，如果跳槽到任何需要处理超过 25000 名个人用户信息的企业，且作为企业的主要股东、首席执行官及负有信息安全责任的高管时，则必须确保该企业已经建立并执行综合信息安全计划，否则将面临高额罚款。[4]

鉴于美国联邦和不同州层面的数据监管法规纷繁复杂，对于和美国具有连接点（例如在美经营或上市，服务面向美国境内自然人）的国内企业来说，尤其是涉及网络平台或 APP 服务（收集、使用、披露或留存美国当地个人信息的），可能无法排除企业高管受到当地法规规制的可能性。这对企业管理层重视及强化网络及数据安全管理提出了进一

[4] https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Decision-and-Order.pdf

步的要求。

四、合规挑战以及专业团队的支持

综上，当发生数据泄露事件时，除监管上报和个人信息主体通知的问题，经历数据泄露的跨国企业可能还面临后续一系列合规挑战，例如 1）响应监管部门的问询；2）对媒体报道或舆论进行适当的回应；3）在内部开展安全漏洞处置和系统防护；4）应对第三方或个人有关数据或个人信息的争议；以及 5）评估监管可能对企业和高管个人的追责等。对于上市企业来说，则还需视泄露事件的具体情况，进一步评估对其财务业绩或运营等其他方面有无重大影响，并根据评估情况向投资者披露。

随着全球监管机构执法经验的增加，联动执法活动的趋势开始出现，企业需要为跨境监管或执法给数据泄露事件处置所带来的额外复杂性做好准备。考虑中国网络安全合规的要求，委托中国律师的参与和协调，将是确保事件处理本身符合中国法律要求，避免引发其他合规问题的必要措施。中国律师的法律支持包括（1）领导或参与跨国企业处理事件响应团队；（2）确保全过程符合中国网络安全和数据安全要求规范；（3）协调外部技术调查、网络安全、公共关系专业团队；（3）准备并协助通知受影响个人；（4）向中国网络安全监管机构报告及配合；（4）协调、准备向跨国企业董事会报告；（5）公共关系及危机处理；（6）回应政府调查；（7）应对集体诉讼。

孙博　合伙人　电话：86- 21 22086216　邮箱地址：sunb@junhe.com
马晓媛　律　师　电话：86- 21 22086114　邮箱地址：maxiaoyuan@junhe.com