通力合规评论 —— 2025 年 6 月
数据泄露莫要慌，合规应对有保障

关于数据安全事件，思科(Cisco)前 CEO 约翰 • 钱伯斯曾说过：“世界上只有两类企业：已经被黑的和不知道自己已经被黑的”。随着近年来越来越多的企业依赖于数字化运营，以及网络技术的发展，这句话得到越来越多的印证。而近期，多个国际知名品牌发生规模不等的个人信息泄露事件，再次给企业敲响了重视数据安全事件应对的警钟。

本月的合规评论，我们结合我们长期协助客户应对数据安全事件的经验，为大家介绍企业最关心的三大问题。

一、 数据安全事件发生后，要不要通知个人?

企业掌握的个人信息泄露了，企业一定是有义务通知个人信息主体的吧?但与大家朴素的认知不同的是，数据安全事件中，企业并不一定要通知相关的个人。

根据《个人信息保护法》第 57 条的规定，在发生数据安全事件后，如果“个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人”。也就是说，个人信息处理者是否有义务通知个人，取决于数据安全事件是否具有危害后果。

1. 如何判断数据安全事件对个人的危害?

那么，如何评估数据安全事件对个人是否具有危害呢?没错，可能你也联想到了《个保法》下一个类似的机制(同时也是合规义务)：个人信息保护影响评估(PIA)。

根据《个保法》，个人信息处理者在进行“对个人权益有重大影响的个人信息处理活动”前应当进行 PIA。PIA 的目的是为了评估数据处理活动对个人信息主体的权益的风险和影响，数据安全事件虽然并不是一项个人信息处理活动，但完全可以用 PIA 的评估逻辑和方法，来评估数据安全事件是否会对个人造成危害。

一个简化的 PIA 评估模型中，通常从以下四个方面来评估危害后果：(1)信息敏感度；(2)风险可能性；(3)危害严重性；及(4)措施有效性。例如，假设一次数据安全事件中，企业泄露的个人信息为员工的姓名、职位、工作邮箱等信息。那么这个评估的过程是：

- 信息敏感度：上述个人信息中，不涉及敏感个人信息，因此信息敏感度低；
- 风险可能性：假设泄露的是明文数据，且数据已经被黑客实际获取或访问，那么存在风险可能性；

- 危害严重性：因为泄露的是非敏感且字段有限的工作相关信息，在没有其他个人信息的前提下，对个人的生命健康财产安全造成危害、或者是对人格尊严造成损害的可能性较低，因此危害严重性为低；
- 措施有效性：如果企业在数据安全事件后能够及时修复导致数据泄露的漏洞，加强员工对于数据泄露后可能面临的危害后果的防范(例如针对可能面临的钓鱼邮件的专项通知和培训)，那么可以认为这些措施可以有效防止数据泄露对于个人的危害。

经过上述的评估，且采取了相应的安全措施后，可以认为数据安全事件不会对个人造成危害，那么企业可以免于通知个人信息主体。但需要注意的是，实践中监管部门对于“有效避免损害”的判断标准通常较为严格，且无论如何，监管部门有权在评估后强制要求企业履行通知义务。因此，企业在判断是否适用此例外条款时务必谨慎，避免判断失误而扩大风险。

2. 如何通知个人?

相反，如果经过评估，数据安全事件可能会对个人造成损害的，那么企业就有义务通知个人，或者如果监管部门认为数据安全事件可能会对个人造成损害的，也会要求企业通知个人。

这种情形下，企业要如何通知个人呢?

原则上而言，企业应当一对一地，通知到每一个受到数据安全事件影响的个人。通常而言，建议企业以书面且可以留痕的方式进行通知，例如邮件、短信、APP 推送/通知等方式。目前较为普遍的是采取短信的方式进行通知。

如果无法做到一对一的通知的，企业应采取合理的方式进行公示，例如，在其 APP 内进行公告，或者通过媒体平台进行公告等。

对个人进行通知时，应当告知如下内容：

- 对于安全事件的简要描述；
- 泄露的个人信息类型和字段；
- 安全事件对于个人的影响；
- 企业已经采取的或将采取的处置措施；
- 对于个人自行防范和减低风险的建议和指引；
- 对个人提供的补救措施或补偿；
- 企业的个人信息保护负责人和保护机构的联系方式

二、 数据安全事件发生后，要不要向监管机构报告?

1. 什么情况下，需要向监管机构报告

很多发生数据安全事件的企业向我们询问，向政府报告数据安全事件是否有人数的“门槛”。很遗憾，《个保法》对于数据安全事件政府报告义务的表述是“发生或者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，并通知履行个人信息保护职责的部门”，可以看出，《个保法》对于数据安全事件的报告并没有“门槛”的设置。

现行的法律法规中，比较接近“门槛”的规定是《公共互联网网络安全突发事件应急预案》中规定的等级最低的“一般事件”，其标准为：“10 万以上互联网用户信息泄露”。

此外，网信办于 2023 年 12 月公布的《网络安全事件报告管理办法(征求意见稿)》(“《报告办法草案》”)中将网络安全事件分为“特别重大”“重大”“较大”“一般”四类，其中，“较大”事件的判定标准之一为“泄露 100 万人以上个人信息”。值得注意的是，《报告办法草案》并未明确规定，对于未达到此标准(即泄露少于 100 万个人信息)的“一般”级别网络安全事件，是否也需要强制报告。现阶段，建议企业仍以《个保法》的要求为准。即，一旦发生个人信息泄露，无论数量多少均应当向监管部门进行报告。为兼顾效率与合规，企业可以首先通过电话等方式向监管部门简要说明情况，然后再根据监管部门的指示(如要求提交书面报告)，补充完善材料。

2. 向监管机构报告的时限是什么

《个保法》要求企业在安全事件发生时“立即”采取补救措施，并通知相关部门和个人，但并未给出“立即”的具体时间定义。《报告办法草案》对此进行了细化，要求对于“较大”及以上级别的安全事件(包括泄露 100 万人以上个人信息的情况)，企业应在事发 1 小时内完成报告。

据此，若安全事件涉及 100 万及以上个人信息的泄露，建议企业于 1 小时内向监管机构报告；对于未达到 100 万规模的安全事件，虽无明确的强制时限，但基于《个保法》“立即”通知的原则，建议企业于可行范围内尽快报告。通常情况下，如果企业能够在 24 小时内进行报告，一般可视为符合时限要求。

3. 境外泄露，境内是否无忧?

需注意，在涉及数据跨境的场景下，即使数据泄露发生在境外，境内主体的报告义务也不能豁免。换言之，即使个人信息通过标准合同等合规途径出境，如果因境外接收方(例如集团总部)的安全疏漏导致信息泄露，境内最初收集并提供个人信息的主体仍需对数据全生命周期负责。监管部门在调查时，有权要求境内主体说明其选择境外合作方时的尽职调查、双方数据出境协议(如标准合同)内容、为保障数据出境安全部署的技术与管理措施，以及事件发生后与境外方面协调应对的情况。

三、 企业应该如何预防数据安全事件?

没有任何一家企业可以 100%避免数据安全事件的发生，但通过采取以下的措施，企业可以最大程度地降低数据安全事件发生的概率。

1. 构建数据安全保护体系

有效的风险管理胜过被动的危机应对。企业应从事前预防、事中监测、事后响应等方面入手，构建全面的数据安全与个人信息保护体系。

1) 制度措施

从制度建设和组织保障层面而言，企业应着力构建、完善以下管理机制:

- 健全内部管理制度: 制定覆盖数据收集、存储、使用、传输、销毁等全生命周期的安全策略，并细化数据分类分级标准、访问控制策略及网络安全应急预案。
- 明确数据安全负责人与管理机构: 设立专门的数据安全负责人和管理团队，并赋予其执行数据安全战略所需的充分权限和资源支持。
- 开展数据安全教育与培训: 定期组织面向全体员工，特别是接触核心或敏感数据岗位的专项培训，提升其安全意识和实际防护技能，帮助员工识别并防范如网络钓鱼等日常工作中的安全风险。
- 个人信息保护影响评估(PIA): 对于处理敏感个人信息、利用个人信息进行自动化决策、大规模对外提供或公开个人信息，以及向境外传输个人信息等高风险数据处理活动，企业在启动前必须主动进行 PIA。这不仅是法定要求，更是企业识别、评估并采取措施减轻潜在数据安全风险的重要手段。
- 贯彻数据最小化: 在数据处理的各个环节，严格遵守数据最小化原则，确保个人信息的收集和处理活动，严格限定在已向用户清晰告知并获得其同意(或符合其他法定合法性基础)的特定处理目的之最小必要范围内，坚决避免过度收集和不必要的处理，从源头上减少数据泄露可能带来的冲击。

2) 技术措施

在技术层面，企业需部署多层次的防护手段。结合行业最佳实践，关键技术措施通常包括:

- **访问控制:** 建立严格的身份验证与权限管理机制，遵循“最小够用”和“权限分离”原则，确保不同角色只能访问其职责所需的数据。
- **加密与去标识化:** 对敏感数据，无论在存储还是传输中，均应采用适当强度的加密技术保护；对外提供数据或进行内部数据分析时，应尽可能采用去标识化或匿名化技术处理，以降低个人信息被重新识别的风险。
- **安全审计与日志记录:** 对所有关键数据处理活动进行记录，并定期进行安全审计，以便在发生安全事件时能够有效追溯原因。
- **漏洞扫描与渗透测试:** 定期对信息系统和应用程序进行安全漏洞扫描与渗透测试，以便及时发现并修补潜在的安全缺陷。
- **入侵检测与防御系统:** 部署防火墙、入侵检测/防御系统(IDS/IPS)、Web 应用防火墙(WAF)等网络安全设备，用以实时监控、识别并有效抵御来自内外部的网络攻击。

- **数据备份与恢复:** 建立可靠的备份机制，并定期演练数据恢复流程，以保证在意外时能迅速、完整恢复数据，保障业务连续性。

2. 供应商管理

根据我们的经验，许多数据安全事件并非发生于企业自身，而是源于第三方供应商或服务商的数据泄露。因此，对外部供应商的有效管理是企业预防数据安全事件的重要环节。具体而言，企业应关注以下几个方面:

1) 审慎选择供应商

合作伊始，审慎选择供应商是第一道关口。企业必须对其进行全面的尽职调查，考察其内部管理体系、技术防护实力、数据安全相关的行业资质认证(例如 ISO 27001/27701 等国际标准认证情况)、过往数据安全事件记录、应急响应机制成熟度，以及(若适用)其自身的合规运营状况。

2) 签署数据处理协议

选定合作方后，应与其签署权责清晰、条款完备的数据处理协议。协议应当明确双方在数据处理活动中的角色与责任，详细约定数据处理的目的、期限、方式、所涉及的个人信息类型与范围、双方需采取的安全保障措施(应不低于企业自身标准和法律法规要求)、数据保密义务、发生数据泄露时的通知与配合机制(例如，要求供应商在约定时间内向企业报告)、企业对供应商的审计权限、供应商的再委托限制(即转包给次级供应商的条件和程序)、违约责任的承担方式，以及合作结束后数据的删除或返还要求等关键条款。

3) 持续监督与审计

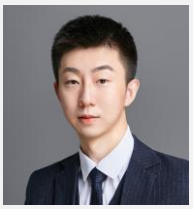
供应商管理并非一劳永逸。企业必须建立并执行覆盖供应商合作全周期的动态监督与审计机制。这包括定期要求供应商提交其数据安全状况证明材料，如最新的安全评估报告、合规认证或第三方独立审计意见等，以此动态评估其安全防护水平。同时，应在数据处理协议中明确企业对供应商数据处理活动的审计权限，以便必要时，通过发放调查问卷、远程系统检查，乃至在遵循保密和最小干扰原则下进行现场核查，以验证其是否持续遵守协议和法规要求。此外，对于供应商可能将其受托处理的数据再次分包给次级供应商的情况，企业应建立严格的事前审批和持续监督机制。通常会要求供应商在进行任何形式的再委托前，必须获得企业的明确书面同意，并确保主供应商通过有约束力的合同条款，将不低于主合同的数据保护标准和义务，有效传递并约束次级供应商。

我们可以提供的与数据安全事件应对相关的法律服务包括:

- 协助企业建立数据安全事件应对所需的制度和流程体系
- 协助企业成立危机应对管理小组(CMT), 确定 CMT 人员职责
- 按照适用法规分类分级标准对安全事件定级, 启动相应处置指导原则与操作规程
- 协助企业履行中国及其他法域法定要求的报告义务
- 协助企业就应急过渡期间的网络安全与服务采购等提供法律服务
- 分析安全事件对企业相关业务合同的影响(是否构成不可抗力、情势变更)并协助企业与合同相对方进行谈判
- 分析安全事件对其他外部利益相关方(例如受影响个人主体)影响并协助企业与相关方进行沟通
- 协助企业与黑客攻击者就赎金勒索等事宜进行谈判
- 协助企业与保险商就网络安全保险进行理赔
- 协助企业应对媒体等第三方的询问质疑
- 协助企业就安全事件导致的法律争议提供法律服务(提起诉讼、应诉、数据出境审查评估)
- 协助企业应对监管部门的现场检查

如有需要, 请随时与我们取得联系:

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



朱晓阳
+86 21 3135 8683
nigel.zhu@llinkslaw.com

往期文章:

AI 也有“署名权”了？简评《人工智能生成合成内容标识办法》
美国对华限制政策新发展——人工智能篇/生物医药篇
简评《生成式人工智能服务管理办法(征求意见稿)》七大问题
隐私计算技术对数据开发利用的突破与限制
AI 不是你想买，想买就能买——从出境合规视角看中美人工智能技术监管
算法推荐 深度合成 生成式 AI？傻傻分不清楚
利好 AIGC 行业？——AIGC 著作权第一案评析

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: **master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野