

通力合规评论 —— 2025 年 8 月 DPO 报送有风险?关注点不该在这儿!

近日, 国家互联网信息办公室发布了《关于开展个人信息保护负责人信息报送工作的公告》, 对《个人信息保护法》第 52 条规定的个人信息保护负责人报送义务进行了细化。针对繁复的报送要求, 许多企业的 DPO 就此向我们表达了“担忧”, 担心在完成政府部门备案登记之后, 企业将面临更严格的监管要求, 而个人将会面临更大的法律风险。但其实, DPO 的履职风险并不来源于报送程序本身, 而完全取决于 DPO 履职行为的规范性和专业性。

那么 DPO 究竟应该怎么当, 才能有效降低甚至规避职业风险, 确保即使完成了备案登记也能从容应对监管要求?本期合规快讯将就此问题进行解读分析。

1. 厘清 DPO 的职责范围

DPO 的职业风险的一大来源为职责的界定不清。如果 DPO 的职责范围过窄, 则有些法定义务没有尽到职责, 可能导致企业合规义务履行的不充分; 而如果 DPO 的职责范围过宽, 则可能导致 DPO 承担本不应该由其承担的职责, 并进而承担法律后果。

对于“DPO 应尽的职责”, 法律层面并没有做出明确的规定。参考国标《信息安全技术 个人信息安全规范》以及我们对于监管实践的理解, DPO 的职责主要包括以下三类:

1) 对于所属企业的职责:

- 统筹个人信息安全工作
- 组织个人信息保护计划并督促落实
- 制定、实施个人信息保护政策
- 建立个人信息清单和授权访问策略
- 开展个人信息保护影响评估, 整改个人信息保护合规风险
- 进行个人信息安全培训

2) 对于个人信息主体的职责:

- 接受、回应个人信息主体对于企业处理个人信息情况的询问、投诉
- 回应个人信息主体的个人信息权利主张

3) 对于监管机构的职责:

- 与监管部门保持沟通, 通报个人信息保护和事件处置情况

可见, DPO 如果没有履行其应尽的职责, 则要么内控制度不健全、要么个人信息主体权利得不到响应, 要么企业与政府之间的沟通脱节, 这都会成为 DPO 执业的风险来源。因此, 企业应当确保 DPO 的工作职责尽可能贴合以上内容, 并通过企业内部制度来予以明确。

2. 对 DPO 提供支持和保障

企业中, DPO 并不是一个人在战斗。个人信息的合规工作也绝非 DPO 一人可以完成。想要 DPO 完全履行其法定职责和义务, 企业必须在多方面给与 DPO 充分的支持与保障, 主要包括:

1) 确保 DPO 的独立性

DPO 中的“O”, 跟 CEO、CFO 中的“O”是同一个“O”, 因此, DPO 应当是管理层成员, 只有这样才能确保 DPO 有足够的权力去调动公司内部资源来实现 DPO 的职责。一些企业因为没人愿意承担 DPO 的责任而让普通员工“挂职”DPO 的做法是不可取的, 可能也无法通过 DPO 的报送。

其次, DPO 最好是独立的职位, 以确保其独立性, 如果一定要兼职, 也建议由法务、合规、隐私保护、信息安全等“后台部门”的负责人担任。应当避免由业务部门(尤其是涉及个人信息处理的业务部门)人员担任 DPO, 以避免业绩和数据合规之间的冲突。

2) 确保 DPO 履职的资源

DPO 履职的资源, 简单来说, 就是权、钱、人。

之所以 DPO 需要是管理层, 就是因为只有管理层成员才有可能调动全公司的资源来实现数据合规。所以, 除了明确界定 DPO 的工作职责外, 明确 DPO 的内部汇报线和管理权限也是非常重要的。

DPO 的工作职责包括督促企业履行法律规定的个人信息保护合规义务(具体见第 3 点), 而这些项目中的大部分需要借助外部专业机构的力量来完成, 因此企业必须确保有充足的预算来支持 DPO 履行合规义务。

人的方面, DPO 应当有一个相对独立的团队, 负责执行 DPO 的指示, 以及与其他部门人员之间的日常对接等。

3) 对于 DPO 的保障与补偿

如果是独任的 DPO, 建议企业考虑其职责及承担的风险, 考虑其薪资及考核/激励机制。如果是兼任的 DPO, 则建议企业考虑职责及风险的增加, 适当考虑增加工资或奖金。

此外, 由于 DPO 可能承担个人法律责任(行政处罚或者民事赔偿), 建议企业为其购买高管责任保险或者 DPO 履职保险。此外, 公司层面也可以考虑网络安全方面的保险, 以降低企业发生数据安全事件等情况下, 企业和 DPO 个人可能承担的风险。

3. 排除企业的个人信息合规风险

即使 DPO 的职责范围再明确, 企业提供的保障再充分, 但归根到底, DPO 的执业风险很大程度上不是来源于其自身, 而是其所属的企业。对于企业的个人信息违法行为, DPO 很难逃脱作为“直接负责的主管人员”, 或者至少是“其他直接责任人员”而被处罚的风险。

因此, DPO 的履职成效很大程度上是结果导向的, 且很可能取决于实际监管行动。即便企业建立了完备的职责体系与完善的制度规范, 如果仍发生违法行为并收到行政处罚, DPO 仍然难辞其咎。

在当前的监管环境下, 我们提示 DPO 们近期重点关注以下环节的风险:

1) APP 个人信息合规

APP(包括小程序、网站等)是大部分企业最重要的营销与销售渠道, 但也是监管机构最容易监管的重点。目前网信、工信、公安等多家监管机构都会定期或不定期对企业的 APP 等进行个人信息合规检测, 并将检测结果进行通告。被通告本身已经是对企业声誉的损害, 而如果企业不能在 30 日内对 APP 完成自测、整改, 则还会面临 APP 下架、罚款等处罚。因此, DPO 们建议务必首先要关注 APP 的个人信息合规情况。

2) 采购/接收数据

近几个月来, 我们多家客户接到公安的调查, 调查的内容均指向为这些客户提供数据的供应商, 以及提供的数据。

许多企业认为, 从第三方采购数据, 即使供应商本身获取数据的来源或者方式有风险, 企业也不会继承这些风险。但其实, 有许多因素会导致企业直接或者间接承担数据供应商违法违规的风险。例如, 如果企业对于供应商收集、处理个人信息的方式和目的做出规定, 那么很可能是被认为企业才是个人信息控制者, 而供应商只是受委托处理个人信息, 从而供应商违法收集/处理个人信息的法律后果将会直接由企业承担。再如, 企业从供应商接收敏感个人信息(例如生物信息、身份信息、行踪轨迹等)的, 由于这些数据的高度敏感性, 企业可能会被推定“明知”数据来源不合规, 从而无法主张“不知情”而免责。

DPO 们必须加强数据供应商的事前(背景调查、资质审查、合同签订)、事中(监督、审计、抽查)、事后(对于数据返回、销毁的核查)审查, 确保企业不为第三方的个人信息违法行为“背锅”。

3) 数据安全事件应对

随着黑客等攻击者的“魔高一丈”, 以及企业内鬼的“防不胜防”, 企业无法完全避免数据安全事件, 只能尽量减小其概率。但对于 DPO 而言, 存在确定性的工作是, 建立、完善企业内部的数据安全事件应对体系。

数据安全事件应对体系包括建立数据安全事件应对小组(建议由 DPO 担任组长); 明确应对小组、企业管理层、部门负责人、普通员工等不同角色在数据安全事件应对中的职责; 明确的数据安全事件内、外部汇报流程; 组织进行数据安全事件演练等等。

此外, 如果真的发生数据安全事件(如个人信息泄露), DPO 应当妥善应对企业的对外通知(个人信息主体)和报告(监管部门)义务。

4) 重点内部合规义务的落实

个人信息合规的法律义务多样而繁杂, 但并非所有合规义务都需要 100% 落实。从“性价比”的角度, 现阶段建议 DPO 关注以下重点个人信息合规义务:

- 各渠道个人信息保护政策的合规、完善与更新
- 个人信息保护影响评估制度的落实与执行
- 个人信息安全事件应急预案
- 个人信息保护合规审计的必要性与实施
- (涉及个人信息的)重要数据的识别、管理、出境评估

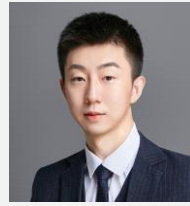
我们如何协助 DPO 更好地进行工作:

- 针对 DPO 的人选、职责、资源配置等提供咨询
- 协助进行 DPO 的政府报送
- 协助制定内部数据合规政策、开展内部网安、数据合规项目
- 协助应对数据安全事件
- 协助应对政府问询和调查
- 针对网络安全相关保险, 审阅保险合同并与保险公司进行谈判
- 对 DPO 日常工作相关的网安、数据合规问题提供支持

如有需要, 请随时与我们联系:



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



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



邓梓珊
+86 21 6043 3793
susan.deng@llinkslaw.com

往期文章:

[敏感个人信息面面观: 身份证号码不属于敏感个人信息了?](#)

[敏感个人信息面面观: 定义、识别准则与实务案例](#)

[敏感个人信息面面观: 概念溯源与域外制度对比](#)

[个人信息出境合规纳入 APP 监管! ——近期 APP 违规通报要点归纳梳理](#)

[买来的数据, 就没风险了?](#)

[AI 也有“署名权”了? 简评《人工智能生成合成内容标识办法》](#)

[靴子落地——个人信息保护合规审计, 你做好准备了吗?](#)

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

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

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

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

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

伦敦

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

免责声明:

本出版物仅供一般性参考, 并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2025