为《通用数据保障条例》做好安排

数据源: 工商月刊 (2018 年 7 月号)
翰宇国际律师事务所合伙人陈晓峰

拥有欧洲客户的香港公司不可忽视欧盟的最新条例

「我们近日已按《通用数据保障条例》更新私隐政策。请按此确认您接受我们最新的私隐政策。」 你的收件箱最近有否被类似的电邮淹没？当你浏览 网页时，有否留意到窗口弹出了大量有关隐私的通知？

在香港，许多人大可不必深究背后原因，直接按下「接受」。然而，这些窗口不断涌现乃因《通用数据保障条例》（GDPR） 这一冗长的新条例近日正式生效，港企绝对不容忽视。

违反 GDPR 最高可被罚款 2,000 万欧元（港币 1.8 亿元），或 公司全球年营业额的 4%（以金额较高者为准）。

GDPR 为欧盟法律下有关数据保障和隐私的条例，于 5 月 25 日生效。

很多港企或会有以下想法：

- 我们的公司不在欧盟，因此 GDPR 与我们无关。
- 不用担心，让欧盟的分公司处理 GDPR 便可。
- 我们的合约不受欧盟成员国的法律约束，因此 GDPR 不适用 于我们。

他们有这些想法亦可以理解，但事实是 GDPR 仍适用于在香 港境外经营的港企。

GDPR 的全球影响

GDPR 有别于其他法例和条例，具有域外效力，其影响遍及全球。

例如，处理有关提供货物及服务或监察自然人行为的资料时，GDPR 适用于处理身在欧盟的自然人之个人资料，即使处理该等数据的人士或公司并不位于欧盟。

例子举隅

在网上销售货品的香港公司：倘在欧盟境外成立的公司透过其官方网站向身在德国的德国公民销售货品，或该网站监察该 德国公民的行为，则该公司须遵守 GDPR。

经营云端服务储存系统的香港公司：例如，客户（部分来自 欧盟）的个人资料提供予香港公司经营的云端服务储存系统。 由于欧盟境内可进入该云端系统，加上该等身在欧盟的人士之个人资料将转移到香港作备存，然后再转移至第三方作进一步处理，因此香港公司处理该等些欧盟人士的个人资料，以及与 该等客户和任何第三方处理者所签订的合约之有关条款，必须符合 GDPR。

谁人受到该条例保障？

港企必须考虑的另一问题为：GDPR 是否适用于所有身处欧盟的人士？

到底 GDPR 只适用于欧盟公民，抑或适用于所有在个人资料被收集时身处欧盟的人士，是备受争议的问题。GDPR 内文列明，条例不仅适用于处理个人资料的欧盟公司，还适用于欧盟境外的公司。看来该条例并不把资料当事人局限于欧盟公民或居民。

就此，各方有不同诠释。为审慎起见，我们建议企业应保持谨慎，假定条例适用于所有在个人资料被收集时身处欧盟的人士，尤其是当公司在全球各地均有业务，并与不同集团公司互 相转移资料。

部分企业或表示并无打算向身在欧盟的人士提供任何服务。就此，条例的适用性将按每宗个案的情况而定，当中的考虑因素包括所涉及的语言（如网上商店有否提供任何欧盟语言）、货币（如价钱是否以欧元标示），以及有否提及任何身处欧盟的顾客。

资料当事人的额外保障

GDPR 赋予数据当事人多项额外权利，包括但不限于反对权、敏感数据的特殊权利、被遗忘权、数据外泄通知，以及详细列明所收集和处理的个人资料类别之需要。此等权利本身极其复杂，本文不在此赘。

GDPR 的实施

GDPR 生效当天，WhatsApp、Facebook、Google 和 Instagram 都卷入因新法例而起的诉讼。Facebook 就被要求罚 款 430 亿美元。苹果、亚马逊和 LinkedIn 等企业亦被起诉，预期更多申诉将陆续有来。

鉴于触犯 GDPR 的潜在风险甚高，我们察觉到部分欧盟境外的企业如《洛杉矶时报》和《今日美国》，已决定封锁欧盟访客。

其他已采取的措施包括要求客户声明自己并非身处欧盟，以及提供不含 cookies 的纯文本版网站，以防在不经意的情况下收集了个人资料。

然而，此举却有如「斩脚趾避沙虫」。事实上，封锁所有欧 盟 IP 能否彻底避免 GDPR 的法律责任仍然成疑。对欧盟这个全球 最大经济体之一避而远之，在商业上也不大合理。

港企的对策？

港企可采取甚么措施，确保遵守 GDPR？

这并不是在数据政策中附加 GDPR 参考数据便可简单了事。（即使没有 GDPR，我们也强烈建议企业根据香港《个人资料(私隐)条例》制订资料私隐政策。）

倘企业与欧盟人士进行任何商业活动或交易，则应就其活动作出评估，以确认是否受到 GDPR 约束。若企业须遵守条例，则应采取一切必要措施，确保该等活动符合 GDPR。

港企可采取的措施包括：

1. 更新数据私隐政策；
2. 确保与附属公司订立适当的合约条款（如把欧盟附属公司持有的雇员资料转移至香港总部，或服务供货商处理欧盟数据 当事人的个人资料）；
3. 修改现有协议，加入 GDPR 所规定的新合约条文，如审计权、委任次级处理者、保安措施等；
4. 就处理者的保安措施及有否遵循 GDPR 展开尽职调查；及
5. 把网站升级至符合 GDPR 标准。在起草设计时，企业应特别 留意相同的通知应否适用于欧盟境外的客户。倘企业能侦测欧盟访客并独立处理他们的数据，则可另外使用欧盟告示。

鉴于 GDPR 已生效，因此如阁下的业务仍未就 GDPR 进行 任何风险评估，则应立即行动，并进行适当的私隐影响评估。