2025 年 7 月及 8 月法规通讯

重大发展

个人资料私隐专员公署（私隐公署）发表两份有关零售行业资料外洩事故调查报告: (A) 光雅珠宝贸易有限公司及爱饰管理有限公司及(B) Adastria Asia Co., Limited。(新闻稿)

(A) 光雅及 *(子公司)* 爱饰事故

两家公司于 2024 年 11 月向私隐专员公署通报资料外洩事故，表示其储存于资料库伺服器的个人资料已被黑客盗取及删除。黑客透过暴力攻击取得一个具系统管理员权限的帐户的帐户凭证。

受影响的**资料当事人**约 **79,400 名**，包括两家公司各自的公司/店铺客户和现职/离职员工。这些资料包括员工姓名、香港身份证号码、出生日期、电话号码、地址及入职日期，以及客户的姓名、香港身份证号码 *(首四位数字或英文字母)*、出生年份及月份、电话号码、电邮地址及会员编号。

主要影响:

私隐公署认为的缺失

- 未有**适时删除离职员工帐户**
- 资讯系统欠缺**有效的保安及侦测措施**
- 伺服器的作业系统已**过时**
- 欠缺资讯保安**政策及指引**
- 未有对资讯系统进行**保安评估及审计**

(B) Adastria事故

总公司在日本的服装零售跨国企业 Adastria,于 2024 年 11 月向私隐公署通报资料外洩事故，表示其客户关系管理及电子商务平台遭受未获授权的第三方入侵。平台由第三方提供，以软件即服务（Software-as-a-Service）方式运作。黑客利用一名现职员工的管理员帐户的帐户凭证连接至平台。

59,205 名客户的个人资料受到了影响。这些资料包括客户的姓名、电话号码及订单资料*（包括交易参考编号、订单日期、会员号码、送货方式、送货/取货日期、送货地址、产品名称与描述，以及价格资料）*。

随后发现，受影响的个人资料于事件发生约两个月后在「暗网」公开，并可供下载。

主要影响：

私隐公署认为的缺失

- **薄弱的密码管理**
- 未有为存取帐户启用**多重认证功能**
- 缺乏**保障个人资料的意识**
- 未有对平台进行适当的**保安检视**

(C) 私隐公署给零售业机构的讯息

私隐专员公署提醒零售行业及持有大量客户个人资料的机构应投放足够资源于网络保安及数据安全。

总的而言，私隐专员公署鼓励机构参考公署刊发的**《资讯及通讯科技的保安措施指引》***(繁体)* 及**《资料外洩事故的处理及通报指引》***(繁体) (可参阅我们23年7月及8月法规通讯)*。 其他有用的资料包括 私隐公署「数据安全」专题网页、「数据安全」热线 （2110 1155），以及「数据安全快测」。

主要影响：

建议的机构性及技术性措施

- 制订**明确**针对资讯系统安全的**内部政策和程序**
  - 并贯彻执行
- 实施**有效措施以预防、侦测及应对网络攻击**
  - 包括定期漏洞扫瞄、以及适时修补保安漏洞
- 停止使用**已被终止支援的软件**，以及**适时更新**
- 加强**密码管理**；采用**多重认证功能**
- 定期进行全面的**保安风险评估及审计**

- 对**第三方供应商提供的服务平台**设置合适的保安功能
  - 并进行**定期的保安检视**
- 制订**资料外洩事故应变计划**
- 为员工提供适当**培训**，提高**数据安全意识**

其他法规发展

ESG：香港可持续发展报告准则

(i)**香港会计师公会已发布**《**香港财务报告准则 S1 及 S2 应用指引- 第 1 部分**》*(英文版)*，作为一份实际应用指引,协助可持续发展及非可持续发展的专业人士应用《香港财务报告准则 S1 号-*可持续相关财务信息披露一般要求*》(HKFRS S1) 及《香港财务报告准则 S2 号-*气候相关披露*》(HKFRS S2)。

监管机构

(ii)**港交所刊发最新的有关股东大会的常见问题及指引**

- **最新的有关股东大会的指引**（标注修订版本）*(繁体)*
  - 更新包括关于**虚拟/混合式股东大会**的指引；最新的代表委任表格式样
- **常见问题 16**（标注修订版本）*(繁体)*
  - 提及**“核心的股东保障水平”**；包括若上市发行人**允许股东在股东大会前以电子方式提交问题，将不会符合**核心的股东保障水平
  - (Q4) *(最新)*《股东大会的指引》指出发行人应作出必要的安排，让**以虚拟方式参与会议的股东**可在会上聆听、发言及实时提出问题
- **常见问题 10**（标注修订版本）*(繁体)*
  - 有关**无纸化机制**的更新，包括无纸证券市场机制 **(USM)** 实施后生效的安排

良治同行

2025年9月