欧洲联盟《通用数据保障条例》

简介

什么是《通用数据保障条例》？

《通用数据保障条例》由欧洲联盟（欧盟）制定，并于2018年5月25日生效，目的是保障欧盟公民的个人资料和提升相关权利。

条例会对谁及如何带来影响？

香港机构即使在欧盟没有设立机关，如在下列情况下处理欧盟人士的个人资料，也可能需遵从《通用数据保障条例》的规定：

1) 向欧盟人士提供（收费或免费）货品或服务；或
2) 监察欧盟人士在欧盟内的行为。

违规会带来什么惩罚？

最高行政罚款可达2,000万欧元或全球年度总营业额的4%，以较高者为准。

重点

域外应用：《通用数据保障条例》适用于在欧盟以外的司法管辖区（包括香港）设立的机构／企业所进行涉及处理个人资料的活动。

「个人资料」的定义：「个人资料」的定义扩大至包括任何有关一名已被识别或可被识别的自然人的资料，例如姓名、地址、身份识别号码、位置资料、网上识别代号，如小型文字档案(cookies)及互联网规约(IP)地址、声音和录像记录、静止图像等。

特别类别的个人资料：「特别类别」的个人资料是指揭示种族或民族本源、政治意见、宗教或哲学信仰、工会会籍的个人资料、有关健康状况的资料或有关一名自然人的性生活或性取向的资料，以及为单独识别一名自然人而处理的基因资料或生物辨识资料。

透明度及同意：《通用数据保障条例》规定资料控制者以清晰简单的语言向资料当事人提供有关处理其个人资料的详尽资讯，并须向他们提供真正及分项的选择，让他们以不含糊的通知或清晰肯定的行动就不同的资料处理活动个别地给予同意。

提升的个人权利：《通用数据保障条例》提升个人各方面的权利。资料当事人有在资料处理方面获通知的权利；个人资料查阅、修改或删除的权利、限制或反对处理的权利、资料可携权，以及不接受以基于自动化处理（包括个人概况汇编）所作决定的权利。

资料外泄及应变：《通用数据保障条例》规定资料控制者向欧盟成员国的监管机构通报资料外泄事故，不可延误（如情况许可，应在得悉事件后不多于72小时内通报）。如有关事故可能对受影响人士的权利及自由造成高度风险，须通知受影响人士，不可延误。

贯彻私隐的设计及预设设定：《通用数据保障条例》规定资料控制者在决定资料处理活动时，实施适当的技术性及机构性措施（例如假名化及数据最少化），以落实执行资料保障原则，并纳入所需的保安措施。

作好准备

机构／企业须 (i) 展示其遵从处理个人资料的原则[1]；(ii) 实施适当的技术性及机构性措施以确保循规[2]；以及 (iii) 在处理的过程中纳入对资料的保障[3]。具体而言，应在资料保障过程中实施或纳入以下措施：

- 委任保障资料主任[4]监督遵从、履行《通用数据保障条例》及作出相关建议；
- 进行资料保障影响评估，以识别及管理资料保障风险；
- 采取贯彻私隐的设计及预设设定，在决定资料处理方法之时，加入所需的保障措施，确保资料保障原则得以落实；
- 为资料处理活动保存记录；以及
- 制定资料处理政策或措施，以展示循规及问责。

*注1, 2, 3：分别根据《通用数据保障条例》第5(2)条、第24条以及第25条。
注4：如处理个人资料不是业务的核心部分和有关活动没有对个人构成风险，若干在《通用数据保障条例》下的责任并不适用，例如委任保障资料主任。

例子

《通用数据保障条例》适用情况

你的机构是一间在欧盟以外成立并于网上营运的小规模高等教育机构，主要以欧盟以内的西班牙语和葡萄牙语大学为对象，并就一些大学课程提供免费意见。学生需要用户名称及密码以取得你的机构的网上材料。学生填妥报名表后，你的机构会提供所需的用户名称及密码。在此情况下，《通用数据保障条例》便会适用。

《通用数据保障条例》不适用情况

你的机构是一个设于欧盟以外的服务提供者，为欧盟以外的客户提供服务。当你的客户到其他国家（包括欧盟国家）旅游时可使用你的服务。假使你的机构没有特别以欧盟人士为服务对象，《通用数据保障条例》便不适用。

延伸阅读

EU GDPR	*https://ec.europa.eu/info/law/law-topic/data-protection_en*
UK ICO	*https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/*
HK PCPD	*https://www.pcpd.org.hk/sc_chi/data_privacy_law/eu/eu.html*