Personal Information Protection Law
Points to Note

The Personal Information Protection Law ("PIPL") (http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml) has been implemented from November 1, 2021. Some points to note are set out below for reference and follow-up:

1. If your offices/work units engage in operations/activities (e.g. teaching and learning, research and human resources management) involving the handling within the Mainland of natural persons' personal information or triggering the provisions of the extra-territorial effect of the PIPL, then your offices/work units need to consider whether and how the PIPL should be complied with. For the application scope of the PIPL, in particular the extra-territorial effect, please note Article 3:

   第三条　在中华人民共和国境内处理自然人个人信息的活动，适用本法。

   在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：
   （一）以向境内自然人提供产品或者服务为目的；
   （二）分析、评估境内自然人的行为；
   （三）法律、行政法规规定的其他情形。

   (An English translation version of the PIPL can be accessed at Stanford DigiChina's webpage: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021)

2. In general, the PIPL is very similar to the GDPR. Hence, for practical and compliance purposes, the PIPL may be regarded as the China version of the GDPR with adjustments in the China setting.

3. For HKU, it seems that, like the GDPR, not many offices/work units will be caught by the PIPL. However, there may still be some risk areas. Hence, colleagues should have some basic understanding and need to do initial assessments within their own offices/work units. Further, the collaboration partners on the Mainland should also work out with HKU the detailed arrangements if the PIPL applies. As and when HKU carries out more Mainland-related operations/activities, the PIPL may be more relevant in regard to compliance.

4. Subject to further consideration and directions of the Central Compliance Team for Personal Data Protection (CCT), the risk-based approach as adopted for the compliance with the GDPR may also apply in regard to the PIPL. In this connection, please refer to HKU's internal GDPR website: https://intraweb.hku.hk/reserved_2/gdpr/index.html and the following:

a. PIPL-related issues should be subject to the governance framework of HKU's ISDM Policy (https://isdm.hku.hk/). In particular, please note the Key Roles and Responsibilities ("the first line of defense").

b. Offices/work units should make a quick and fit-for-purpose assessment as to whether the PIPL may affect their operations/activities, and identify the potential risk areas.

c. If PIPL is relevant and/or risk areas are identified, further consideration and advice about the implementation of the PIPL will be required. Affected offices/work units may form a common task force to use resources and share knowhow more efficiently and effectively, including designating staff members to receive more training and to seek formal legal advice from Mainland qualified lawyers. For general training, focus group discussion or initial risk assessment exercise, please contact the Data and Security Team, ITS (email: hkuisdm@hku.hk).

d. The affected offices/work units should review their relevant operations/activities, and design an implementation plan for compliance with the PIPL as required.

External training information about the PIPL may be received from the PCPD, law firms and other outside bodies, and such information will be collected and can be accessed by **CLICKING HERE**.

For further discussing issues about the PIPL, please make an appointment with the Data and Security Team, ITS (email: hkuisdm@hku.hk).

University Data Protection Officer

Updated: November 2023