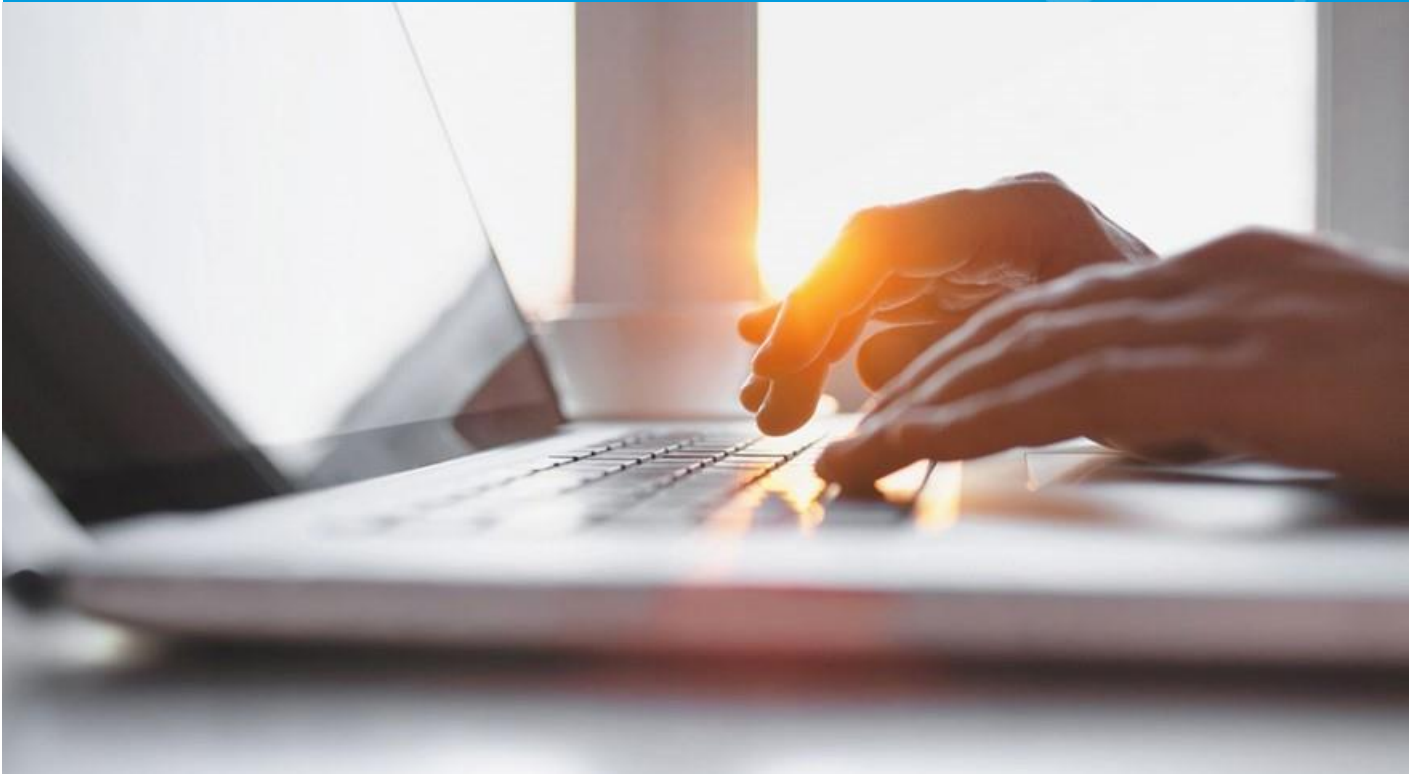


2022 年 7 月

## 为中国大陆人士提供服务的香港企业：需要考虑的个人资料问题



### 简介

于 2021 年 11 月 1 日生效的《个人信息保护法》是中华人民共和国内地（「**中国**」）第一份完全关乎个人资料保护和隐私的法案。由于《个人信息保护法》具有域外效力，《个人信息保护法》不仅适用于在中国境内运作的企业，也适用于（1）为中国境内的自然人提供产品或服务及（2）分析或评估中国境内自然人活动的企业。因此，许多企业（包括香港特别行政区（「**香港**」）境内的企业）都需要遵守原属司法管辖区的数据隐私法以及《个人信息保护法》。

在此客户通报内，本所从香港及中国法律的角度探讨了一些个人资料问题（这些问题对于在香港营业并向中国境内人士提供服务的企业特别重要）。香港的主要数据保护法例是《个人资料（私隐）条例》（「**私隐条例**」）。于本客户通报探讨事宜中国法律仍在发展中，并在不久的未来可能改变。

《个人信息保护法》使用「个人信息」这个词语，而《私隐条例》则使用「个人资料」表达。本所将在此客户通报中采用相同的字词。

## 1. 中国境外及香港的企业是否要遵守中国的《个人信息保护法》及香港的《私隐条例》？

### 《个人信息保护法》

如上所述，如「**个人信息处理者**」（即根据《个人信息保护法》负责处理个人信息的实体）为了以下目的而处理个人信息，都必须遵守《个人信息保护法》：

- (a) 向中国境内自然人提供产品或服务；或
- (b) 分析或评估中国境内自然人的行为。

如果您的企业位于中国境外，无论您是否在中国境内设立商业实体，出于上述目的处理中国境内自然人的个人信息，则您必须在中国境内设立一家专门机构或指定一位代表，并将该机构名称或代表姓名、联系方式等的重要信息提交予负责执行个人信息保护职责的相关部门。

### 《私隐条例》

相比之下，《私隐条例》并无规定其域外适用范围。行政上诉委员会在 2020 年的谷歌案件中确认了这一点。因此，《私隐条例》仅适用于在或从香港境内控制、持有、处理或使用个人资料的实体。有别于《个人信息保护法》，即使位于香港境外的企业在收集香港境内人士的个人资料，该企业都不需要遵守《私隐条例》。

## 2. 企业就处理个人信息/数据取得个人同意后应注意什么？

### 《个人信息保护法》

根据《个人信息保护法》，如果（1）个人信息的处理目的、（2）处理个人信息的方式和（3）处理的个人信息种类发生任何变更，个人信息处理者必须通知个人并**重新**取得个人同意。

此外，《个人信息保护法》还要求个人信息处理者在以下的特殊情况下取得个人的单独及额外同意：

- (a) 向第三方提供个人信息；
- (b) 向中国境外的一方提供个人信息；或
- (c) 处理一旦泄露能导致侵犯人格尊严或对自然人或财产造成伤害的个人信息（「**敏感个人信息**」）。

个人信息处理者还应注意，除法律或行政法规另有规定外，所收集的任何个人信息只能保留到处理目的所需的最短期限（「**保存期**」）。个人信息处理者还需提供便捷的途径，让个人可随时撤回同意权。如果发生以下任何一种情况，则个人信息处理者必须主动删除相关的个人信息：

- (1) 保存期限已经届满；
- (2) 处理信息的目的已实现，无法实现或为实现处理目的不再必要；
- (3) 个人已撤回其同意；或
- (4) 个人信息处理者已停止提供产品或服务。

## 《私隐条例》

类似于《个人信息保护法》，如果收集的個人資料用于新目的，则负责收集、持有、处理或使用个人资料的企业（「**数据用户**」）一般需要重新获得被收集个人资料的个人同意（根据《私隐条例》称为「**资料当事人**」）（受若干豁免）。此外，如果个人资料随后使用于直接促销，数据用户必须获得数据当事人的同意或表示不反对。

与《个人信息保护法》不同的是，如原本授予的同意足够清晰并涵盖以下情况，则数据用户毋须取得额外个别同意：

（1）将个人资料转移予第三方；（2）将个人资料转移至香港境外；或（3）处理「敏感」个人资料（《私隐条例》不区分敏感及非敏感个人资料）。尽管如此，如出现上述情况，香港个人资料私隐专员公署（「**香港私隐署**」）建议数据用户将上述事项通知数据当事人。

《私隐条例》亦声明，数据用户保留个人资料的时间不得超过为达到收集个人资料的目的而所需的时间。个人也有权提供书面通知向数据用户撤回其同意，但并不代表数据用户有义务删除相关的个人资料。

## 总结

由于《个人信息保护法》将某一类个人信息指定为敏感个人信息及对跨境个人信息转移实施更严格的管制，一般而言中国的个人信息保护制度要求高于香港。企业应注意，资料当事人在《个人信息保护法》下可撤回其同意，此时该企业必须停止收集和处理他/她的个人信息，并且删除相关的个人信息。

### 3. 企业应如何处理员工的个人信息/数据？

#### 《个人信息保护法》

如果企业必须处理员工个人信息以订立或履行员工一方当事人的合同，或必须按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理，《个人信息保护法》容许企业在未取得个人同意的情况下处理个人信息。本所建议企业在劳动合同和规章制度中加入个人信息相关的条款、将个人信息的收集和处理规范化并根据需要及要求员工在入职时或入职后签署必要的授权。

由于企业的日常经营过程中会涉及到企业与其客户或各类贸易伙伴之间个人信息的流转，企业应（1）以书面形式向第三方澄清个人信息有关的权利及义务；（2）制定私隐政策去说明企业对其收集的个人信息承担的责任；及（3）就员工在开展业务过程中处理个人信息相关事提供行为指引。

#### 《私隐条例》

对待员工个人资料应与对待任何其他个人的资料一样（《私隐条例》并没有关于员工个人资料的特别规例）。与收集任何其他人士的个人资料一样，雇主应向其员工提供个人资料收集声明，告知员工将会收集的個人資料的类型，其用途以及受让人的类别等。

企业还应制定私隐政策声明。香港私隐署亦提倡企业应制定私隐管理系统，数据保护视为企业管治的一部分。香港私隐署在2019年3月发布了私隐管理系统的最佳行事方式指引。香港私隐署其中一项建议是，数据用户应委任一名保障数据主任去监督企业遵守《私隐条例》及私隐管理计划，为员工提供有关数据保护的最新培训及教育。

## 总结

企业应在其雇佣合同中包含有关个人信息/资料的条款，并要求员工在加入公司时同意收集必要的个人信息/资料。企业还应制定私隐政策并确保其员工在有关收集个人信息/信息方面接受良好的培训。

### 4. 违反《个人信息保护法》及《私隐条例》会有什么后果？

#### 《个人信息保护法》

违反《个人信息保护法》规定的企业可受到行政处罚、承担民事和刑事责任。行政处罚包括（1）责令改正或警告；（2）没收违法所得；及（3）最高处 5000 万元人民币以下或上一年度营业额 5% 的罚款。企业甚至可能被责令暂停或终止相关业务，而通报相关主管部门吊销相关业务许可或吊销营业执照。负有直接责任的人员还可被限制在一定期限内担任相关公司的董事、监事、高级管理人员或个人信息保护负责人。

如果企业侵犯了个人的个人信息权益，且不能证明其没有过错，则该企业需要承担民事责任从而须向有关人士赔偿个人遭受的任何损失或企业因而获得的任何利润。如果任何违反行为构成刑事犯罪，企业也可被追究刑事责任。

#### 《私隐条例》

在香港，违反《私隐条例》条文最高罚款港币 1,000,000 元及监禁 5 年。违例例子包括在未经数据当事人同意的情况下使用数据当事人的个人资料直接营销或披露数据当事人的个人资料。

此外，如果香港私隐署收到投诉或有合理原因相信有违反《私隐条例》的行为，其可进行调查。如调查发现确实有违反《私隐条例》的行为，香港私隐署会发出执法通知书，指示应采取的补救或预防措施。如不遵守执行通知书，可被判罚款高达港币 50,000 元（首次定罪）或港币 100,000 元（其后定罪）及监禁两年。

如违反《私隐条例》导致数据当事人遭受任何损失或损害，数据用户亦可能须承担民事法律责任。

## 建议

为确保遵守《个人信息保护法》及《私隐条例》以避免该等处罚，企业需要制定关于个人资料的适用内部政策、实施及执行该政策、并定期检讨该政策以确保遵守各司法管辖区的最新资料私隐及保护法例。如果发生数据泄露，本所建议企业立即收集信息评估对数据当事人的影响，联络相关执法机构，并采取适当的预防/补救措施。本所还建议数据用户就此数据泄露情况告知相关的数据当事人。

### 5. 符合了 GDPR 要求的文件是否也符合《个人信息保护法》及《私隐条例》的要求？

虽然这三个制度之间有些相似之处，但遵守 **GDPR** 并不等同于遵守《个人信息保护法》和/或《私隐条例》。根据 GDPR 制定的任何规则或政策都应根据《个人信息保护法》及《私隐条例》重新审视。

## 6. 个人信息/信息的跨境传输有哪些要求？

### 《个人信息保护法》

虽然《个人信息保护法》没有确立个人信息跨境转移的法律定义，但我们认为以下两种情况均构成个人信息的跨境转移：

- (a) 在中国境内收集的个人信息转移至了中国境外；及
- (b) 中国境外的企业能够使用或处置存储于中国境内的个人信息。

在出现跨境转移个人信息的情况下，《个人信息保护法》要求企业取得相关个人的单独同意并采取某些措施，例如进行安全评估或个人信息保护认证、组织安全审计和个人信息保护影响评估，与境外接收方签订合同（网信部门制定的标准合同）约定双方的权利义务等。

### 《私隐条例》

相比之下，由于《私隐条例》第 33 条（禁止除在指明情况外将个人资料移转至香港以外地方）尚未生效，现时香港并无个人资料跨境转移限制。目前尚不清楚第 33 条何时生效，但当第 33 条生效后，企业只有在满足以下要求之一的情况下才可将个人资料转移到香港境外：

- (1) 个人资料转至的地方具有与《私隐条例》大体上相似的任何法律；
- (2) 资料当事人已以书面同意跨境转移；
- (3) 数据用户有合理原因相信 (a) 转移是为了避免针对资料当事人的不利行动或减轻该等行动的影响而作出的、(b) 获取数据当事人的书面同意是不切实际的、及 (c) 如获取资料当事人的书面同意是切实可行的，资料当事人是会给予上述同意的；
- (4) 跨境转移数据属于《私隐条例》第 33 条的豁免之一；或
- (5) 数据用户已采取一切合理的预防措施，并已进行一切尽职审查，以确保所收集的個人資料不会以违反《私隐条例》的方式处理。

一般情况下，第二个要求是最容易满足的，因数据用户可在收集有关数据当事人的个人资料时提供的收集个人资料声明中要求资料当事人同意个人资料的跨境转移。

为筹备第 33 条，香港私隐署建议数据用户检讨其数据转移安排，透过内部信息屏障等措施控制跨境数据流动，保存转移至香港境外的个人资料的清单，并定期进行审计和检查。亦建议数据用户通知个人关于任何拟议的跨境资料转移，并使其数据处理活动透明化。与《个人信息保护法》一样，企业也应与海外接收者依个人资料的转让方和受让人的权利和义务签订合同，即使到目前为止，香港政府尚未规定标准合同。

## 总结

《个人信息保护法》对控制和处理个人信息的企业施加了新的一套义务。与《私隐条例》一样，它也以同意为前题，尽管标准更严格。最重要的是，《个人信息保护法》具有域外效力，而《私隐条例》则没有，因此企业应重新审视和审查

其与数据相关的政策和流程，以确保遵守适用的法律规则。如果两套或以上的信息/数据保护法律之间有冲突，则应遵守持有更严格标准的立法。

未来《个人信息保护法》一些细节将如何诠释和执行仍有待观察。

### **我们给予的协助**

我们经常依照中国和香港的信息/数据保护制度向客户提供建议。我们能协助您的企业全面遵守《私隐条例》和《个人信息保护法》规定的所有义务。我们亦有其他地区的办公室能依照其他司法管辖区的信息/数据保护法（如 GDPR）提供建议。

## 联系我们



### 廖雅明

合伙人，融资组负责人

电话：+852 2533 2717

电邮：katherine.liu@shlegal.com



### 周红

合伙人 - 伟途律师事务所\*

电话：+86 20 8388 0590

电邮：zoe.zhou@shlegalworld.com



### 黄军融

律师

电话：+852 3166 6933

电邮：james.wong@shlegal.com

\*广东伟途律师事务所（注册地为广州的中国律师事务所）和罗夏信律师事务所（注册地为香港的律师事务所）根据《关于建立更紧密经贸关系的安排》设立了“罗夏信律师事务所-广东伟途律师事务所联营”。《关于建立更紧密经贸关系的安排》是一个中国大陆和香港之间的自由贸易协定。在此框架下，香港的律师事务所与内地律师事务所联营，并依据中国和非中国的法律在中国大陆提供全面的法律服务。

罗夏信律师事务所在全球拥有超过1100名员工，其中包括190多位合伙人，致力于为我们的客户达成商业目标——客户包括上市及私人企业、各大机构和个人。

我们的团队集合了才思敏捷的专业人员，能够满足客户的需求，在最恰当的时机由最适当的人员为客户提供最恰如其分的建议。秉承法律人才的最高标准，从而解决最复杂的问题，我们为客户针对实际情况，提供实用而专业的建议。

我们的总部设在伦敦，并在亚洲、欧洲和中东地区设有八个办事处。不仅如此，我们还与其他顶级的律所建立了紧密的联系。凭借多元化的专业知识和多重文化，我们不仅对当地的情况有更强的洞察力，同时也有能力提供无缝的国际化服务。