# 同意的制度分野与规则适配
## ——以《个人信息保护法》为基准的 GDPR、PDPA 比较考察

作者：杨迅 | 李依然 | 张莹

“同意”(consent)同时出现在中国《个人信息保护法》(PIPL)、欧盟《通用数据保护条例》(GDPR)与新加坡《个人数据保护法》(PDPA)之中，且均被列为个人信息处理的合法性基础之一。但是，相同的用语却有不同的含义：三法对同意的功能定位、构成要件与适用边界存在系统性差异。

本文以 PIPL 为分析基准，考察 GDPR 与 PDPA 项下“同意”的制度逻辑及其在典型场景中的运行效果。

## 一. 同意的制度语境、适用条件与形式要求

正如著名历史法学派大儒萨维尼所说“法并非主权者命令的结果，而是源于民族精神……是对民族精神或民族共同意识的表达。”各国的个人信息保护立法也体现着相关群体的集体意志。因此，同样的“同意”作为合法处理个人信息的基础，也呈现不同的运行机制。

三法共用“同意”一词，其规范含义却由各自的制度语境所塑造：GDPR 中，“同意”是被严格审查并降格处置的基本权利表达；PDPA 中，“同意”是被交易理性重构的商业确认；PIPL 中，“同意”是被法定主义羁束的兜底授权。以 PIPL 为基准的比较显示，PIPL 的同意制度在形式上最为精细——单独同意、书面同意、告知清单均有明确的操作规范，可审计性与可问责性较强；但在结构性不对等关系中的实质保护上存在缺口，自愿性审查机制的缺位使同意的保护功能高度依赖形式要件的执行效果。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

### (一) 不同文化背景下的“同意”机制

个人信息保护语境下“同意”的功能差异，源于三法不同的生成背景与规范定位。

PIPL 以法定主义为核心，“同意”提供了兜底的合法性基础。PIPL 第 13 条以封闭式列举穷尽个人信息处理的合法性事由，除末项“法律、行政法规规定的其他情形”外，未设置类似 GDPR“合法利益”的一般弹性条款，体现鲜明的法定主义立场：处理正当性首要来源于法律明文授权与公共监管框架，而非私人合意。在此结构中，“同意”承担双重功能：作为列举事由中唯一源于私人意思的正当化通道，它为立法未及覆盖的商业场景保留合规出口；“同意”又被严格羁束于法定框架之内，在敏感个人信息、跨境传输等场景升格为单独同意或书面同意。由于“合法利益”事由缺位，当个人信息的处理无法归入 PIPL 第 13 条的其他事由时，“同意”在实务中事实上充当兜底依据，成为 PIPL 严格法定体系中唯一的灵活性来源——这是理解中国法下同意泛化现象的规范基础。

GDPR 诞生于欧洲普遍的个人权利意识，将数据保护定位为基本权利(《欧盟基本权利宪章》第 8 条[1])，其规范预设是：个人信息的处理正当性来源于法律对相互冲突之利益与基本权利的权衡，而非个人对每一项处理的逐案授权。据此，GDPR 第 6 条第 1 款[2]将同意降格为六项合法性基础之一，且非优先选项。这一安排看似悖反：同意的构成要件被抬至最高水准，制度优先级却被刻意压低。其规范逻辑在于：若同意在结构性不对等关系中容易取得、难以验证，以其作为默认基础反而削弱保护——形式上的授权将掩盖实质上的支配。故 GDPR 以”抬高门槛＋降低顺位”组合处置“同意”：常规处理优先诉诸合同必要、法定义务与合法利益三项合法性基础，“同意”保留给真正由个人自主决定的场景。

---

[1] Charter of Fundamental Rights of the European Union, Article 8 — Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

[2] GDPR Art. 6 Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a)the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b)processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f)processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

新加坡的个人信息保护立法带有深深的重商主义烙印。PDPA 除了以保护个人信息为目标，也同样体现了对商业习惯的尊重。PDPA 第 13 条[3]以同意为处理起点，但第 15 条、第 15A 条分别以“视为同意”(deemed consent)、“经通知视为同意”(deemed consent by notification)大幅扩张其外延：自愿提供、合同必要、通知后未反对三类情形均可成立有效同意，沉默与不作为原则上不构成障碍。其规范逻辑并非意思表示理论，而是理性商事主体的交易预期：只要处理符合交易情境中理性人的合理预期，法律即以“同意”之名确认其正当性。这是新加坡商业导向立法的必然产物——作为高度依赖转口贸易与跨国服务的开放经济体，新加坡须将数据流动的制度成本降至最低，“同意”由此被重构为以客观交易理性为标尺的合理性审查框架，而非对个人意思的规范性要求。

### (二) 适用条件与执行限制

三法的不同文化背景和立法理念，决定了“同意”作为处理个人信息的基础，有着不同的适用条件，其执行也受到不同的限制。

从构成要件来说，GDPR 对同意设定自由作出、具体、知情、明确四重要件(第 4 条第 11 项[4])，第 7 条[5]另规定举证责任、同意请求的呈现形式、禁止捆绑与撤回规则。“具体”要求同意指向特定目的，概括授权原则上无效；“自由”在雇佣、公共服务等不对等场景中发挥排除功能，即如果双方的实际地位不对等，那么个人主体给出的同意是否满足“自由”要件则会受到质疑。

---

[3] Personal Data Protection Act 2012, Article 13: Consent required: An organisation must not, on or after 2 July 2014, collect, use or disclose personal data about an individual unless —
(a) the individual gives, or is deemed to have given, his or her consent under this Act to the collection, use or disclosure, as the case may be; or
(b) the collection, use or disclosure (as the case may be) without the individual's consent is required or authorised under this Act or any other written law.

[4] GDPR Art. 6 (11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

[5] GDPR Art. 7 Conditions for consent
1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. 2Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. 2The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 3Prior to giving consent, the data subject shall be informed thereof. 4It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

相比而言，PIPL 第 14 条要求“同意”在“充分知情的前提下自愿、明确作出”。“自愿”主要通过禁止捆绑式同意落实——提供服务不得一揽子要求同意处理与核心功能无关的个人信息，但 PIPL 未建立针对不对等关系的实质性自愿审查机制，审查重心落于告知充分性与形式合规性。而 PDPA 不设“自由”、“明确”等实质性要件，控制功能转由第 18 条[6]目的限制承担：收集、使用与披露须限于理性人在具体情境下认为适当的目的。不难看出，三法的控制结构不同：GDPR 审查“同意是否真实”，PIPL 审查“形式是否齐备”，PDPA 审查“目的是否合理”。

无论是 PIPL，GDPR 还是 PDPA，“同意”并非合法处理个人信息的唯一条件。PDPA 以目的适当性限制同意的形式上的广度，换而言之，即使获得相关个人信息主体的同意，该个人信息处理活动也必须以适当的目的为限；PIPL 将目的明确性与处理必要性(第 6 条)作为独立义务，对敏感个人信息另设"特定目的与充分必要性"要求(第 28 条)，因此在 PIPL 下处理个人信息的，需要满足多重的合规要求；GDPR 则以数据最小化(第 5 条第 1 款第(c)项)为基本原则，即无论是获得相关个人信息主体的同意，还是满足其他合法性基础的要求，处理个人信息的范围、时间和方式必须以最小必要为原则。可见，相对于 PIPL 而言，PDPA 下个人信息处理活动的弹性空间更大，只需满足合理性要求，而 GDPR 下处理个人信息的范围更小，需要限制在严格最小范围之内。

### (三) 形式要求

三法在同意的形式上也各不相同。

PDPA 对“同意”持有开放态度，不设统一形式门槛，明示、默示与三类“视为同意”并存，甚至经通知之后不作反对，也可被认为是“同意”的一种形式。

PIPL 采取梯度化安排，重视同意的形式考察：一般处理适用一般同意，敏感个人信息(第 29 条)、向境外提供(第 39 条)适用单独同意或书面同意；相关国家标准将弹窗确认、禁止预勾选等操作细则化，使同意形式高度可审计、可取证——形式要件发达与实质审查薄弱并存，构成 PIPL 同意制度的显著特征。

GDPR 以实质要件吸收形式问题：第 9 条对特殊类别数据要求“明确同意”(explicit consent)，须以声明或清晰肯定行为作出——预勾选框、沉默均不构成有效同意；同意是否有效，最终取决于个人信息主体是否有决定给出“同意”的真实的自由。

## 二. 雇佣场景下的合法性基础配置

劳动雇佣场景中如何适配处理员工个人信息的合法性基础，体现了三法的不同理念。

[6] Personal Data Protection Act 2012, Article 18 Limitation of purpose and extent:
An organisation may collect, use or disclose personal data about an individual only for purposes —
(a) that a reasonable person would consider appropriate in the circumstances; and
(b) that the individual has been informed of under section 20, if applicable.

### (一) 三法对雇佣场景的不同理解

雇佣关系是检验同意制度的试金石：雇员对雇主存在人身与经济的双重从属，同意的自由性与真实性在此可能受到质疑。三法的理解路径不同，导出差异化的合法性基础配置。

GDPR 对劳动雇佣场景下的“自由同意”采取不信任立场。GDPR 序言第 43 条[7]指出，控制者与数据主体之间的显著不对等是判断同意是否自由的重要因素；第 7 条第 4 款要求审查获取同意是否构成提供服务的条件。在雇佣从属之下，雇员“同意”极可能沦为权力关系的法律外衣而非真实意思自治。故雇佣场景的常规处理原则上排除同意，而以第 6 条的合同必要、法定义务与合法利益事由承接，并通过第 88 条授权成员国制定劳动数据保护特别规则。

PDPA 从商业理性出发，将日常人事管理视为劳动关系的固有内容。新加坡个人数据保护委员会(PDPC)认可雇主为订立、管理或终止雇佣关系的合理相关目的处理员工数据，无需逐一取得同意。其规范理由是：常规人事处理属于理性雇员缔结合同时即可合理预期的管理范畴，保护需求由第 18 条目的限制与理性人标准承接——审查对象不是“雇员是否同意”，而是“处理是否落入雇佣管理的合理边界”。同意仅在目的超出雇佣范畴(如官网发布员工照片、用于无关营销)时适用。

PIPL 持有法定主义立场。PIPL 第 13 条第(二)项将人力资源管理权限锚定于“订立、履行个人作为一方当事人的合同所必需”与“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所必需”，处理正当性来自法律授权与制度性依据，而非雇佣关系的默示合意。同时，PIPL 未设 GDPR 式的自愿性排除机制，雇员在从属地位下作出的单独同意，其效力在规范上不受质疑。其结果是：人力资源管理构成法定的处理个人信息的合法性基础，其边界由“必要性”与“依法”限定；“同意”同时作为处理个人信息的兜底基础，可以作为处理员工个人信息的扩张场景。

### (二) 典型处理事项的合法性基础匹配

以下总结劳动雇佣场景下，依据三法，处理员工个人信息的常见合法性基础。

1. 薪资发放与银行账户信息。此事项在三法下的合法性基础基本是一致的：GDPR 项下依第 6 条第 1 款第(b)项(履行合同所必需)，必要时结合第 88 条转化的成员国劳动立法义务(归入第(c)项)；PDPA 项下由雇佣例外与合同必要之视为同意覆盖；PIPL 项下直接援引第 13 条第(二)项的履行劳动合同的必要范围。

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), OJ L 119, 4.5.2016, p. 1–88, Recital (43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

2. 考勤与门禁管理。处理一般考勤信息，三法均不强制要求同意。分歧出现在生物识别信息的升级处理：以指纹或人脸替代打卡时，GDPR 项下生物识别数据属特殊类别数据(第 9 条)，但考勤门禁通常可经第 9 条第 2 款第(b)项(履行劳动法与社会保障法项下义务)处理，无须诉诸员工同意；PDPA 项下落入雇佣管理例外的合理边界。PIPL 项下生物识别信息属敏感个人信息，须具备特定目的与充分必要性并取得单独同意(第 28、29 条)——考勤管理本身可依第 13 条第(二)项处理一般信息，一旦升级为指纹打卡即触发单独同意义务。这是 PIPL 的突出实务痛点：管理惯例的微小升级即产生单独同意义务，而在不对等关系中单独同意的保护效力最弱，其功能主要是满足审计与问责要求。
3. 招聘与背景调查。GDPR 项下，处理候选人主动提交的信息可依托第 6 条第 1 款第(b)项(缔约前的必要措施)；背景调查涉及向第三方核实，超出缔约必要范围时须另行寻找合法性基础，同意在求职者场景中的自由性同样存疑。PDPA 项下，求职者主动提交的信息可用于应聘评估，由于是招聘的合理必要流程，可以以“视为同意”作为合法性基础。PIPL 项下，第 13 条第(二)项可覆盖常规招聘，但背景调查、候选人信息共享给集团其他实体等超出订约必要范围，因无合法利益事由可援引，只能回到同意的合法性基础，涉及敏感个人信息的还需单独同意。
4. 对外发布。官网发布员工照片、员工活动宣传等超出雇佣管理边界的事项，可能都需要额外的同意，但是有着不同的限制和条件：GDPR 要求同意必须真正可选，拒绝不得带来不利后果，否则应转向合法利益基础；PDPA 因目的超出雇佣例外需单独合规判断，需要考察在扩大的“雇佣管理”场景下，该等处理活动是否合理；PIPL 同样认为该等处理活动超出人力资源管理法定边界，只能以同意兜底，涉及向第三方提供的还需“单独同意”。

由上述配置可见：在处理员工个人信息的问题上，GDPR 较少依赖员工的个人同意，而尽可能依赖“履行合同所必需”、“正当利益”等基础；PDPA 更多依赖明示和暗示的“同意基础”，以商业和理性为限定；而 PIPL 虽然也有“履行合同”和“劳动管理”的合法性基础，同时也提供“同意”基础作为扩充。

## 三. 跨境传输场景的监管机制与个体同意的配置

个人信息主体的“同意”在跨境传输中也有重要法律意义，体现三法的不同立法意图。

### (一) 三法跨境规则的建构逻辑

跨境传输规则最清晰地呈现三法的制度定位差异，其建构逻辑可由各法对跨境风险的预设解释。

GDPR 以“保护水准不因跨境而稀释”为轴心。其规范预设是自身构成全球最高保护标准，跨境流动的核心风险在于接收法域保护不足导致权利保障落空。故第五章以第 45 条充分性认定与第 46 条适当保障(标准合同条款、约束性企业规则)为常规路径，制度重心在于以法律机制锁定接收方义务，确保保护标准的等价性。

PDPA 同样以等效保护为出发点(第 26 条[8]), 但服务于商业连续性的政策目标。作为转口贸易与区域服务枢纽, 新加坡将常态化跨境流动视为跨国经营的固有内容, 而非需要逐案审批的例外。故第 26 条的等效保护主要通过机构间法律约束机制一次性实现, 覆盖集团内部流转与跨境服务外包等常态场景, 个人同意仅为例外选项——制度重心在于以一次性的机制安排替代逐案个体授权。

PIPL 的跨境规则呈现公法监管主导形态。第 38 条确立安全评估、认证与标准合同三条出境路径, 均嵌入行政监管程序(申报、审查、备案); 第 40 条对关键信息基础设施运营者与达到规定处理量的处理者施加强制出境评估。其规范重心在于维护国家数据安全与数据主权, 跨境传输被预设为需要公权力审查的高风险行为, 个人层面的控制仅作为补充性要求。

### (二) 跨境传输中“同意”的地位与作用

在三法下, 个人信息主体“同意”在数据跨境传输中的地位各不相同。

GDPR 第 49 条将同意列为跨境传输的例外事由(derogation), 适用受三重限制: 其一, 告知标准升格, 数据主体须在被告知缺乏充分性认定与适当保障、传输存在风险的前提下明确作出同意; 其二, 解释上从严, EDPB 指南明确该条仅适用于偶发、个别、非系统性传输, 不得作为常态化流动的通道; 其三, 功能上补充, 例外事由的定位是填补刚性机制无法覆盖的缝隙。典型适例仅限于为接收临时外派员工一次性传输少量信息, 或应数据主体本人请求向其境外账户传输数据。由此, 同意在 GDPR 跨境规则中的地位是“最后手段的例外”(exceptional)——非常态、高门槛、补充性。

PDPA 跨境规则中, 同意仅为若干合规选项之一, 但实践价值有限: 面对集团内部常态化数据流动, 以逐人同意替代机制安排既不必要也不经济, 标准条款等机制工具可一次性覆盖持续性传输。“同意”的“残留”功能仅在传输对象零散、难以建立机制覆盖的场景(如向境外猎头披露个别候选人信息)中存续。

PIPL 下, 按照第 39 条“同意”要求, 无论选择第 38 条项下何种出境路径, 处理者均须向个人告知境外接收方名称、联系方式、处理目的与方式、个人信息种类及行权方式等事项, 并取得单独

[8] Personal Data Protection Act 2012, Article 26 Transfer of personal data outside Singapore

(1) An organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.

(2) The Commission may, on the application of any organisation, by written notice exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation.

(3) An exemption under subsection (2) —

(a) may be granted subject to such conditions as the Commission may specify in writing; and

(b) need not be published in the Gazette and may be revoked at any time by the Commission.

(4) The Commission may at any time add to, vary or revoke any condition imposed under this section.

同意。单独同意并非监管机制的替代，而是监管审查的必备前提要件。其功能主要是程序性确认而非风险控制：实操中，个人在冗长的跨境告知文本中作出“知情”判断的能力有限。尤其在间接获取个人信息的场景——如制造商拟将经销商收集的用户信息向境外关联主体传输——企业缺乏触达终端个人的有效渠道，单独同意履行成本显著上升，合规价值主要是满足审计留痕要求。

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**


| 上海 | 北京 | 深圳 |
| --- | --- | --- |
| 上海市银城中路 68 号<br>时代金融中心 19 楼<br>T: +86 21 3135 8666<br>F: +86 21 3135 8600 | 北京市朝阳区光华东里 8 号<br>中海广场中楼 30 层<br>T: +86 10 5081 3888<br>F: +86 10 5081 3866 | 深圳市南山区科苑南路 2666 号<br>中国华润大厦 18 楼<br>T: +86 755 3391 7666<br>F: +86 755 3391 7668 |
| **香港** | **伦敦** | |
| 香港中环遮打道 18 号<br>历山大厦 32 楼 3201 室<br>T: +852 2592 1978<br>F: +852 2868 0883 | 1/F, 3 More London Riverside<br>London SE1 2RE<br>T: +44 (0)20 3283 4337<br>D: +44 (0)20 3283 4323 | |


**www.llinkslaw.com**

**Wechat: LlinksLaw**

**本土化资源 国际化视野**

免责声明:
本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2026