汉坤法律评述

2019 年 3 月 12 日

漢坤律師事務所
HAN KUN LAW OFFICES

北京 | 上海 | 深圳 | 香港

透明和控制：从近期动态看个人信息保护合规重点

作者：段志超 | 蔡克蒙 | 何雯

2019 年 2 月 1 日，全国信息安全标准化技术委员会公布了《信息安全技术个人信息安全规范》（“**《个人信息安全规范》**”）的修订草案（“**《规范草案》**”），向社会公开征求意见。3 月 1 日，App 违法违规收集使用个人信息专项治理工作组[1]发布了《App 违法违规收集使用个人信息自评估指南》（“**《评估指南》**”）。分别作为个人信息保护合规的重要实践指南以及四部委组织开展的 APP 违法违规收集使用个人信息专项治理行动的重要参照，这两部实操规范虽然各有侧重，但都针对了前期个人信息保护领域中暴露出的突出问题，体现了监管部门进一步加强个人信息保护执法力度的趋势。

本文尝试以下列三个运营中常见的问题为中心，总结和梳理《规范草案》和《评估指南》中的相关规定，在为企业合规提供指南的同时也对可能出现的问题进行探讨。

一、收集：什么样的个人信息可以收集？

《规范草案》和《评估指南》都着力于从必要性的角度对企业过度收集个人信息进行约束。具体而言，其都意图将个人信息的收集和细分的业务功能对应，并规定不得通过捆绑业务功能来获得用户对个人信息收集和使用的概括同意。此外，《规范草案》还在现行《个人信息安全规范》的基础上对基本业务功能和扩展业务功能做了更具操作性的划分指引，并对于不同类型的业务功能获得用户同意的方式和对应的处理方式做了不同的规定。

（一） 以业务功能为基础映射收集的个人信息，禁止业务功能的强制捆绑和一揽子授权

监管机构显然对现行实践中企业将所有业务功能捆绑在一起获取同意，以在满足《网络安全法》对同意的最低限度要求的前提下尽可能多的收集个人信息的做法有所察觉，并意图对其进行规制。

其中，《规范草案》和《评估指南》都明确规定，企业需要将每一项业务功能对应收集的个人信息列明，并以业务功能为基础分别获取用户的同意，而不得通过捆绑产品或服务的方式来强迫用户一次性授权企业收集多个业务功能所对应的多种类型的个人信息。

作为更加具体和可操作的指引，《评估指南》更是明确要求逐项列明业务功能和每一项业务功能对

[1] 根据中央网信办、工业和信息化部、公安部、市场监管总局在 1 月 23 日发布的《关于开展 App 违法违规收集使用个人信息专项治理的公告》，全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会成立 App 违法违规收集使用个人信息专项治理工作组，制定该指南。

应收集的个人信息类型，而排除使用概括说明的方式，为个人信息合规工作提出了高标准。

《规范草案》	《评估指南》
5.3 不得强迫收集个人信息的要求 当产品或服务提供多项需收集个人信息的业务功能时，个人信息控制者不得违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求。对个人信息控制者的要求包括： (a). 不得通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意各项业务功能收集个人信息的请求… **5.4 收集个人信息时的授权同意** 对个人信息控制者的要求包括： (a). 收集个人信息前，应向个人信息主体明确告知所提供产品或服务的不同业务功能分别收集的个人信息类型，以及收集、使用个人信息的规则（例如收集和使用个人信息的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等），并获得个人信息主体的授权同意…	**5．是否明示收集个人信息的业务功能** 隐私政策中应当将收集个人信息的业务功能逐项列举，不应使用“等、例如”字样。 **6．业务功能与所收集个人信息类型是否一一对应** 隐私政策中对每个业务功能都应说明其所收集的个人信息类型，不应出现多个业务功能对应一类个人信息的情况。 **7．是否明示各项业务功能所收集的个人信息类型** 每个业务功能在说明其所收集的个人信息类型时，应在隐私政策中逐项列举，不应使用“等、例如”等方式概括说明。 **24．是否存在将多项业务功能和权限打包，要求用户一揽子接受的情形** 1、 不应通过捆绑 App 多项业务功能的方式，要求用户一次性接受并授权同意多项业务功能收集个人信息的请求。 2、 根据用户主动填写、点击、勾选等自主行为，作为产品或服务的业务功能开启或开始收集个人信息的条件。

（二） 为区分基本业务功能和核心业务功能提供客观化标准，仅在退出机制上对两者进行区分

虽然现行《个人信息安全规范》已经尝试就核心业务功能和附加业务功能进行区分，以解决业务功能强行捆绑的问题。但实践中，企业通常会就业务功能的定义做不同的解读，以尽可能地扩大核心功能的范围，从而使得其获取不同类型的个人信息的行为合法化和正当化。

针对该问题，《规范草案》做了更具有操作性的设计和规定。一方面，其为基本业务功能（对应核心业务功能）和扩展业务功能（对应附加业务功能）的划分提供了更具有操作性的指引。另一方面，其也整体提升了对个人信息收集同意的标准，仅是在用户拒绝提供相关同意的退出机制上针对不同类型的业务功能做出了不同的规定[2]。

[2] 《规范草案》附录 C.2：“基本业务功能的告知和明示同意…个人信息主体不同意收集基本业务功能收集所必要的个人信息时，个人信息控制者可拒绝向个人信息主体提供该业务功能。”《规范草案》附录 C.3：“扩展业务功能的告知和明示同意…b)如个人信息主体不同意收集扩展业务功能收集所必要的个人信息，个人信息控制者不得反复征求个人信息主体的同

在基本业务功能和扩展业务功能的划分上，《规划草案》强调了用户对产品的期待等客观因素，且弱化了企业可控的版本迭代，体验提升等主观因素。此举旨在增加划分的可预测性，为执法提供更确实的标准。在退出机制上，其规定仅在用户拒绝针对核心业务功能提供必要的个人信息时企业可拒绝提供相关服务，而在用户仅拒绝就扩展业务功能提供相关信息时，不得影响其使用基本业务功能，以希籍此进一步减少业务功能和个人信息采集的捆绑问题。

上述规定也在《评估指南》中有所体现，其规定对于对应于基本业务功能之外的业务功能的个人信息的收集需经过用户自主选择同意，对于和业务功能无关的个人信息，企业不得收集。

《规范草案》	《评估指南》
C.1 区分基本业务功能和扩展业务功能 保障个人信息主体选择同意权，首先需划分产品或服务的基本业务功能和扩展业务功能，划分的方法如下： (a). 应根据个人信息主体选择、使用所提供产品或服务的根本期待和最主要的需求，划定产品或服务的基本业务功能； (b). 不应将改善服务质量、提升用户体验、研发新产品单独作为基本业务功能； (c). 将产品或服务所提供的基本业务功能之外的其他功能，划定为扩展业务功能。	**26. 收集与业务功能有关的非必要信息，是否经用户自主选择同意** 当 App 运营者收集的个人信息超出必要信息范围时，应向用户明示所收集个人信息目的并经用户自主选择同意。 **27. 是否收集与业务功能无关的个人信息** App 不应收集与业务功能无任何关系的个人信息。

<u>探讨和后续关注</u>

尽管《规范草案》和《评估指南》已经就解决个人信息收集必要性的问题做出了多维度和具有可操作性的设计，实践中，在基本业务功能和扩展业务功能界定等问题上，仍然可能出现不同主体的不同解读。就此，我们注意到全国信息安全标准化技术委员会正在制定相关的指引方案，以进一步明确十类基本功能的具体内容，为企业提供更切实和确定的合规依据[3]。

需要注意的是，如相关指引对基本功能及其对应的必要个人信息仅限定在较小的范围，根据《规范草案》和《评估指南》的规定，企业在收集扩展功能对应的个人信息时，需要在其启动时逐项明示以获取用户的同意，实践中该操作可能会在用户体验和业务设计上给企业提出更多的挑战。

二、应用：基于画像的个性化展示应该注意什么？

近年来，基于用户画像的个性化推送以及与其相关联的精准广告营销引起了越来越多人的注意。从用户

意。除非个人信息主体主动选择开启扩展业务功能，在 24 小时内向用户征求同意的次数不得超过一次；c) 如个人信息主体不同意收集扩展业务功能收集所必要的个人信息，不得拒绝提供基本业务功能或降低基本业务功能的服务质量”。

[3] 《DPO 沙龙纪实：个人信息安全规范修订中的用户授权与个性化推送》

角度观察，个性化推送的滥用可能会影响其获取信息的效率或间接影响其作出不正确的判断，继而侵害其正当权益。在此背景下，《规范草案》和《评估指南》均强化了对个性化展示的透明度及用户控制力方面的要求。

《规范草案》和《评估指南》重申了现行法规中企业就画像以及与之相关的个性化展示需要向用户进行充分说明并获取其同意的规定，要求企业在隐私政策中说明个人信息用于用户画像、个性化展示的应用场景和对用户可能产生的影响。在此基础上，《规范草案》还要求对基于个性化展示推送的内容做显著的标示，增强用户对基于其个人信息的使用的了解。

进一步地，《规范草案》还明确要求企业在进行个性化展示的同时提供简单直观的非个性化展示选项和退出途径。即，让用户有权控制是否被基于其画像推送相关内容或进行搜索结果排序。此外，《规范草案》还以倡议的方式建议企业赋予用户对其画像的更高的控制权，以及在用户决定退出个性化展示的同时向其提供删除相关画像标签或个人信息的选项，这点也和《评估指南》中关于隐私政策应向用户提供撤回已同意的授权的规定相对应。

《规范草案》	《评估指南》
7.4 个性化展示及退出 对个人信息控制者的要求包括： (a). 在向个人信息主体推送新闻或信息服务的过程中使用个性化展示的，应： (1) 以显著方式标明“个性化展示”或“定推”等字样； (2) 为个人信息主体提供简单直观的退出个性化展示模式的选项。 (b). 电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项； (c). 在向个人信息主体提供业务功能的过程中使用个性化展示的，宜： (1) 建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关程度的能力； (2) 当个人信息主体选择退出个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。	**11．个人信息的使用规则** 如果 App 运营者将个人信息用于用户画像、个性化展示等，隐私政策中应说明其应用场景和可能对用户产生的影响。 **15．用户权利保障机制** 隐私政策应对以下用户操作方法提供明确说明： 1、 个人信息查询 2、 个人信息更正 3、 个人信息删除 4、 用户账户注销 5、 撤回已同意的授权

探讨和后续关注

一个有待探讨的重点问题是个性化展示的范围。《规范草案》第 3.15 条将个性化展示界定为“基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。”然而，实践中常见的基于用户群体标签开展的个性化展示是否属于个性化展示？例如，基于用户收入范围、所在城市、可能感兴趣的内容等用户群标签对具有该标签的特定用户群体进行推送是否构成《规范草案》项下的个性化推送？从《规范草案》的文本来看，似乎只有信息来源和推送对象均为同一人的推送才构成个性化展示，因此答案可能是否定的。在这种情况下个性化展示的范围无疑将大大限缩，这一立场是否会为规范终稿所采纳仍有待观察。

三、合作：第三方合作中的数据合规要求是什么？

《规范草案》在原《个人信息安全规范》的基础上进一步完善了对第三方数据处理的合规要求，将第三方个人信息处理活动分为委托第三方处理个人信息、第三方构成共同控制者，以及企业接入或跳转的第三方产品或服务三类。这三类第三方处理情况的核心区别不在于采取特定的技术手段上的差异，而是在于企业与第三方之间关于个人信息处理的范围、目的等决定权的分配。

- 在企业委托第三方处理个人信息的情况下，委托企业决定个人信息处理的目的和范围，受托第三方应按照企业指示处理个人信息。此时，第三方仅构成个人信息处理者。例如 APP 运营者在应用程序中部署第三方统计分析类的 SDK，第三方完全按照 APP 运营者的指令将个人信息用于统计分析并反馈分析结果，不会另行使用或共享相关个人信息。

- 企业与第三方共同决定个人信息处理的范围和目的的情况下，第三方可能构成个人信息共同控制者。例如在 APP 中嵌入第三方广告 SDK 或 APP 中嵌入第三方地图服务商 API 接口，往往双方共同决定 SDK 收集哪些信息或对 API 接口开放哪些信息。

- 企业将服务接入或跳转至第三方产品或服务，第三方通常对个人信息处理的范围和目的享有决定权。例如通过企业的账号登录第三方服务。

实践中第三方个人信息处理监管的重点和难点在于第二种和第三种情况。

在企业嵌入第三方插件或向第三方开放接口的情况下，常见的问题包括企业未就第三方信息收集对用户进行告知取得用户同意，或在第三方超出服务所必需的范围收集个人信息或变更个人信息使用目的的情况下仅取得用户的概括式授权同意。甚至企业往往对其嵌入的第三方插件收集或通过 API 接口向第三方传输的个人信息的情况缺乏标记和记录，导致隐秘收集个人信息的情况泛滥，难以对第三方进行有效管理和追责。对此，《评估指南》和《规范草案》要求企业向用户明确告知第三方收集个人信息的情况并取得用户同意。由于《规范草案》提高了对扩展业务功能的告知和同意要求，这意味着如果嵌入第三方仅提供或支持扩展业务功能，则应就第三方提供的扩展业务功能进行逐项说明并取得用户明示同意。

在企业将服务接入或跳转至第三方服务的情况下，实践中企业往往未明确标明或区分服务由第三方提供，未能对第三方进行有效的审查和监督。对此，《规范草案》要求企业在事前建立第三方产品或服务接入管理机制，并在接入后对第三方产品和服务进行持续监督。首先，企业应明确标明接入的产品或服务由第三方提供。在接入前，企业应建立第三方产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件。企业还应通过合同等形式明确双方的安全责任及应实施的个人信息安全措施，并要求第三方向个人信息主体征得收集个人信息的授权同意，建立响应个人信息主体请求、申诉等的机制。在接入期间，企业应妥善留存平台第三方接入有关合同和管理记录，应督促和监督第三方产品或服务提供者加强个人信

息安全管理。如企业发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入。

《规范草案》	《评估指南》
8.7 第三方接入管理 当个人信息控制者在其产品或服务中接入具备收集个人信息功能的第三方产品或服务且不适用本标准 8.1 和 8.6[4]的，对个人信息控制者的要求包括: (a). 应建立第三方产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件； (b). 应与第三方产品或服务提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施； (c). 应向个人信息主体明确标识产品或服务由第三方提供； (d). 应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅； (e). 应要求第三方根据本标准相关规定要求向个人信息主体征得收集个人信息的授权同意，核验其实现本项要求的方式； (f). 应要求第三方产品或服务建立响应个人信息主体请求、申诉等的机制，并妥善留存、及时更新，确保个人信息主体查询、使用； (g). 应督促和监督第三方产品或服务提供者加强个人信息安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入； (h). 涉及第三方嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的，宜： (1) 开展技术检测确保其个人信息收集、使用行为符合约定要求； (2) 宜对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超出约定行为的及时切断接入。	**14．对外共享、转让、公开披露个人信息规则** 如果存在个人信息对外共享、转让、公开披露等情况，隐私政策中应明确以下内容： 1、 对外共享、转让、公开披露个人信息的目的； 2、 涉及的个人信息类型； 3、 接收方类型或身份。 **22．若存在嵌入第三方代码插件收集个人信息的功能，是否向用户明示** 如果通过嵌入第三方代码、插件等方式将个人信息传输至第三方服务器，应通过弹窗提示等方式明确告知用户。

探讨和后续关注

《规范草案》对企业嵌入第三方插件或接入第三方产品或服务提出了很高的合规要求。如这些要求全部施行，那么企业需要对嵌入或接入的第三方进行排查和评估，根据排查评估修订隐私政策及弹窗交互式界

[4] 第 8.1 条指委托处理的情况；第 8.6 条指共同个人信息处理者的情况，由于《规范草案》未对这两部分进行实质性修改，故我们未在此引用相关条文。

面，完善对用户的告知和同意机制，并升级产品或服务，剔除或停止接入不符合要求的第三方插件、产品或服务。企业还可能需要与第三方签署或修订相关合作协议，落实第三方的个人信息安全责任以及企业对第三方的监督检查权利。这些要求可能给企业带来很大挑战，例如平台方往往接入众多第三方产品或服务，平台方可能难以具备足够的资源和能力审核并持续监督第三方同意的获取情况以及用户权利请求响应机制的运转状态，或对第三方开展技术检测。企业究竟对第三方负有何种程度的审查监督义务仍有待实践检验。

结语

数字经济下，个人信息和大数据的价值被越来越多的企业所认知。而基于用户画像的自动决策和个性化推送在为企业提高效率和带来利益的同时，也加剧了信息传播的不对称性，切实影响到用户的体验和利益。个人信息收集和应用过程的黑盒化只能加剧用户和企业之间的对立。透明和控制，即便短期内会给企业带来较多的合规负担，从长远利益考量，才是数据合规和个人信息保护中不变的解药。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系。

段志超

电话： +86-10-8516 4123
Email： kevin.duan@hankunlaw.com