君合专题研究报告君
JUNHE

2021 年 3 月 15 日

App 合规系列—企业收集使用个人信息时如何取得同意（上）

前言

随着移动互联网应用程序（以下简称“**App**”）在各行各业中的应用趋于广泛，其中蕴含的个人信息保护问题也不断引起企业和用户的关注。其中，企业通过App收集使用个人信息的过程中，取得用户同意是非常重要的一环，需要企业在合规层面予以高度重视。例如，如何取得用户同意，在什么情况下需要取得用户的同意，是否存在某些情况不需要取得用户的同意，对于一些特殊群体和信息如未成年人、生物识别信息、敏感信息等应当如何处理，在取得同意这一问题上需要注意哪些合规问题点等，都值得企业深思熟虑，反复推敲。本文分上下两篇，旨在对企业如何取得用户同意这一问题的合规要点进行梳理和总结，以期对企业通过App收集使用个人信息的合规实务有所助益。

一、关于同意的境内外相关立法

从国外立法动向来看，欧盟的《一般数据保护条例》（General Data Protection Regulation，以下简称“**GDPR**”）对于数据主体“同意”相关的各方面问题做了非常细致的规定。关于同意的核心条款主要是第6（1）条的（a）点[1]和第9（2）条的（a）点[2]。除此之外，第7条（同意的条件）、第8条（信息社会服务中适用儿童同意的条件）、第17条（被遗忘权）、第18条（限制处理权）、第20条（数据携带权）等均有与数据主体同意相关的内容。

从国内立法动向来看，《民法典》、《网络安全法》中均有对于取得同意的相关规定。《民法典》第一千零三十五条规定，处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外。《网络安全法》规定，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。未经被收集者同意，不得向他人提供个人信息。此外，《信息安全技术 个人信息安全规范》（以下简称“**《个人信息安全规范》**”）、《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南》、《儿童个人信息网络保护规定》等法律法规中均对取得同意做出了更为细致的规定。最后，《信息安全技术 个人信息告知同意指南（征求意见稿）》（以下简称“**《告知同意指南》**”）针对告知同意的规则以及各个场景下的告知同意方法做出了非常详尽的规定，值得企业在制定用户协议和隐私政策时予以参考。

二、同意的定义和类别

根据GDPR第4条，数据主体的“同意”指的是数据主体通过一个声明，或者通过某项清晰的确信行动而自由作出的、充分知悉的、不含混的、表明同意对其相关个人数据进行处理的意愿。

根据中国相关法律法规，同意的类别包括明示

[1] GDPR 第 6（1）条的（a）点的相关内容如下：1. 只有满足至少以下一项条件时，处理才是合法的，且处理的合法性仅限于满足条件内的处理：(a)数据主体已经同意基于一项或多项目的而对其个人数据进行处理。

[2] GDPR 第 9（2）条的（a）点的相关内容如下：1. 对于那些显示种族或民族背景、政治观念、宗教或哲学信仰或工会成员的个人数据、基因数据、为了特定识别自然人的生物性识别数据、以及和自然人健康、个人性生活或性取向相关的数据，应当禁止处理。2. 如果具有如下条件之一，第 1 段将不适用：(a)数据主体明确同意基于一个或多个特定目的而授权处理其个人数据，但依照欧盟或成员国的法律规定，数据主体无权解除第 1 段中所规定的禁令的除外。

同意和授权同意。其中，“明示同意”指的是个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。其中，肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

而“授权同意”指的是个人信息主体对其个人信息进行特定处理作出明确授权的行为，这既包括通过积极的行为作出授权（即明示同意），也包括通过消极的不作为而作出授权（如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。根据《告知同意指南》，个人信息主体未自行拒绝使用产品或服务，且产品或服务可通过公开可访问的隐私政策等文件了解收集使用个人信息规则的情况也属于授权同意的范畴。

同时，与“同意”密切相关的一个行为是“告知”。个人信息控制者（本文中主要针对收集使用个人信息的企业）在收集个人信息之前，应当将与个人信息处理活动相关信息提供给个人信息主体，使其了解个人信息处理活动的有关规则。这一行为在《告知同意指南》中定义为“告知”。告知是同意的前提，企业在告知时应当遵循告知同意的基本原则，考虑相关要素以及业务的特殊场景要求，确保告知同意过程合法合规。

三、告知同意的基本原则

根据《个人信息安全规范》，个人信息控制者开展个人信息处理活动应遵循合法、正当、必要的原则。根据《告知同意指南》，告知与同意分别有以下基本原则，个人信息控制者在实施告知同意时应当考虑以下基本原则，以保证告知过程和征得同意过程均为切实有效。

行为	原则	细则
告知	公开透明	公布收集、使用个人信息的范围、目的，不隐瞒产品或服务所收集的个人信息及其使用目的，不采取故意遮挡、隐藏等方式诱导个人信息主体略过告知内容。
	逐一传达	向个人信息主体逐一告知相关内容，有显著困难时也可采取公告方式。
	同步实时	当涉及具体业务功能收集、使用等个人信息处理场景时，或触发个人信息收集行为时，对个人信息主体进行即时告知。
	真实准确	反映产品或服务真实、准确的个人信息收集使用范围、目的。
	具体明确	告知个人信息的类型、目的等内容需结合实际业务场景，不使用格式化条款。
	清晰易懂	告知文本符合个人信息主体的语言习惯（如简体中文），使用标准化语言、数字、图示等，避免使用有歧义的语言。
同意	告知一致	征得同意的授权范围与所告知内容相一致。
	自主选择	主动向个人信息主体展示征得同意的选项，支持其自行做出选择，不给出同意时，仅影响当前服务类型的正常使用。
	时机恰当	在个人信息收集行为发生前，且同步传达告知内容时，征得个人信息主体同意，以增进个人信息主体对业务功能与所收集的个人信息之间关联性的理解。
	分类独立	区分产品或服务的服务类型后，分别征得个人信息主体同意，不采用捆绑方式强迫个人信息主体一次性接受或拒绝所有可能收集的个人信息。

四、告知同意需考虑的要素

根据《告知同意指南》，个人信息控制者在实施告知同意时还可以考虑以下五个要素，优化告知同意的方案和机制。

五、取得何种同意及如何取得同意

（一）明示同意优先、授权同意例外

如前所述同意包括明示同意和授权同意两种类别。根据《告知同意指南》，个人信息控制者在征得个人信息主体同意时，应当优先采用明示同意，确保个人信息主体的意愿表示是在理解收集目的和相关处理规则的基础上自主给出的、具体的、清晰明确的，且尽量避免采取授权同意的机制，因为此类机制可能导致个人信息主体忽略对个人信息处理规则的关注。

在某些条件受限或成本巨大等情况下且经个人信息影响评估后无高风险，才可考虑采用授权同意的模式。这些情况包括以下几种：

a) 产品或服务的业务场景网络等环境条件受限；

b) 产品或服务的展示界面和展示方式受限；

c) 基于最小必要考虑，为实现业务功能仅收集无法直接关联到个人身份的个人信息；

d) 执行同意需要付出大额成本才可以实现；

e) 告知后执行同意可能对个人信息主体使用产品或服务的良好习惯带来削减；

f) 告知后执行同意可能影响业务运营安全的；

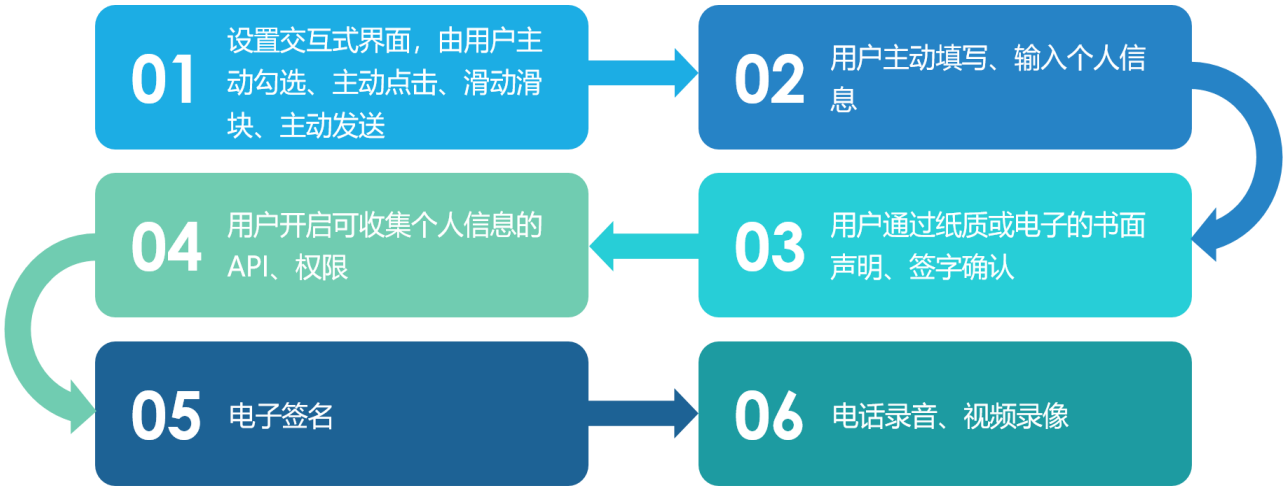
g) 需告知的目的等内容有助于保护个人信息主体权益；

h) 需告知的目的等内容属于免于告知同意的情形的[3]。

（二）取得明示同意的模式选择

明示同意的模式主要包括以下六种，个人信息控制者可以结合产品或服务的特点，选择上述同意模式中的一种或几种。例如，如果收集个人信息可能对个人信息主体权益造成重大财产损失的，可以在交互式界面执行主动勾选、点击等操作基础上（01），进一步采取电话录音（06）、签字确认（03）等方式。

[3] 具体请参见《信息安全技术 个人信息告知同意指南（征求意见稿）》第六章的内容。



六、何种情况下需要取得同意

根据《告知同意指南》，告知同意有四种主要的适用情形，分别是收集使用个人信息时、使用目的变更时、对外提供个人信息时以及其他情形。这四种情况的具体情形如下表所示：

适用情形	要求	具体情形
收集使用个人信息时	需向个人信息主体告知收集、使用个人信息的类型、目的、方式和范围，并征得个人信息主体的明示同意。	a） 个人信息主体主动填写、选择、上传等主动提供个人信息的； b） 个人信息控制者通过智能终端、API、SDK、IoT 设备、浏览器、传感器等自动采集个人信息的； c） 个人信息控制者通过与用户交互记录个人信息主体行为的； d） 个人信息控制者从第三方间接接受、查询等方式间接获取的； e） 个人信息控制者从非完全公开渠道搜集个人信息的； f） 个人信息控制者从个人信息主体关联身份或账号收集个人信息的； g） 个人信息控制者使用大数据、AI 等技术分析、关联和生成个人信息的。
使用目的变更时	需向个人信息主体告知涉及的个人信息类型、变更原因、变更后的处理目的，并再次征得个人信息主体的明示同意。	a） 个人信息控制者收集个人信息后，超出原有授权范围应用于新的业务场景的； b） 个人信息控制者间接获取个人信息后，进行加工处理形成新的个人信息并用于其他目的； c） 个人信息控制者所提供的产品或服务基于业务扩展而增加的新的功能，该新增功能收集使用个人信息都超出原授权范围的； d） 个人信息控制者进行收购、兼并等，将获取的个人信息超出原有授权范围使用的； e） 个人信息控制者收集后涉及重大处理规则变化的，例如需要将个人信息传输到境外进行处理的。
对外提供个人信息时	需向个人信息主体告知个人信息类型、目的、接收方等，并事先征得个人信息主体的明示同意。	a） 个人信息控制者应业务所需向第三方共享个人信息； b） 个人信息控制者应业务变更等原因，向第三方转让个人信息，且不再保留个人信息； c） 个人信息控制者以不定向方式向公众公开披露个人信息； d） 其他个人信息控制者对外提供个人信息的情形，但个人信息控制者向接受其委托、为其提供个人信息处理服务的情形除外。
其他情形	需向个人信息主体告知原因、目的、处理方式、可能产生的影响等内容。	a） 涉及个人信息出境的情形； b） 个人信息处理规则，如隐私政策，内容发生对个人信息主体权益产生影响的实质性变化时； c） 个人信息主体撤回授权同意时；

		d） 个人信息主体注销账号时； e） 对个人信息进行汇聚融合，且可能对个人信息主体权益产生影响时； f） 发生个人信息安全事件，且可能对个人信息主体合法权益造成侵害时。

七、取得同意的例外

根据《个人信息安全规范》，在某些情形中，个人信息控制者收集、使用个人信息不必征得个人信息主体的授权同意以及明示同意，即存在一些免于告知同意的情形，具体如下所示：

a) 与个人信息控制者履行法律法规规定的义务相关的；

b) 与国家安全、国防安全直接相关的；

c) 与公共安全、公共卫生、重大公共利益直接相关的；

d) 与刑事侦查、起诉、审判和判决执行等直接相关的；

e) 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；

f) 所涉及的个人信息是个人信息主体自行向社会公众公开的；

g) 根据个人信息主体要求签订和履行合同[4]所必需的；

h) 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；

i) 维护所提供产品或服务的安全稳定运行所必需的，如发现、处置产品或服务的故障；

j) 个人信息控制者为新闻单位，且其开展合法的新闻报道所必需的；

k) 个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的。

除此之外，《告知同意指南》中针对收集使用个人信息时、使用目的变更时、对外提供个人信息时免于告知同意的情形做了更为详细的规定，具体请参考该指南第六章的相关内容。

结语

本篇主要阐述了关于同意的境内外相关立法、同意的定义和类别、原则、模式、适用情形以及例外，重点回答了如何取得同意、什么情况下需要取得同意、取得同意的例外这几个关键问题，希望能对企业从原则和基本规则上把握收集使用个人信息时的合规要点有所帮助。对于与App中取得同意相关的具体规则、特殊领域的同意规则、相关的罚则和处罚案例、给企业的合规建议等，我们将在下篇进行详细阐述，敬请期待。

[4] 个人信息保护政策的主要功能为公开个人信息控制者收集、使用个人信息范围和规则，不宜将其视为合同。

（本页无正文）

杨锦文　合伙人　电话：86 10 8553 7608　邮箱地址：yangjw@junhe.com
高　健　律　师　电话：86 10 8519 1359　邮箱地址：gaojian@junhe.com
李圆圆　律　师　电话：86 10 8540 8665　邮箱地址：liyuanyuan@junhe.com