君合专题研究报告 JUNHE

2021 年 3 月 24 日

App 合规系列——企业收集使用个人信息时如何取得同意（下）

前言

上篇对于关于同意的境内外相关立法、同意的定义和类别、原则、模式、适用情形以及例外等原则和基本规则做了阐述，本篇旨在对于针对违反告知同意规则的App通报、与App中取得同意相关的具体规则、特殊领域的同意规则、相关罚则、给企业的合规建议等具体的问题和规则进行梳理和分析，以期对企业在具体业务中收集使用个人信息时，包括出台用户协议和隐私政策时的合规实务有所助益。

一、针对违反告知同意规则的App通报

对于App违法违规收集使用个人信息的问题，相关监管部门设置了相应的用户举报渠道（例如App违法违规收集使用个人信息治理工作组设置了公众号“App个人信息举报”和网站pip.tc260.org.cn，中央网信办设置了违法和不良信息举报中心，中国互联网协会受工业和信息化部委托设置了网络不良与垃圾信息举报受理中心等）接受用户投诉举报并进行相应处理，并不定期公示通报违法违规收集使用个人信息的App名单。

目前仍存在大量App违反告知同意规则收集个人信息的行为。例如，2020年App违法违规收集使用个人信息治理工作组曾通过“App个人信息举报”公众号和网站通告了177款App违法违规收集使用个人信息，我们选取了其中违反告知同意规则的通报案例归纳整理如下表，供企业对照自身情况参考：

序号	App 名称	违反告知同意规则收集使用个人信息的情况
1.	某博客 App	以不正当方式误导用户同意收集个人信息：在隐私政策中以“在你发送微博、使用微博提供的位置定位服务时，我们会收集你的位置信息、设备信息”为由收集用户设备信息。
2.	某房产中介 App	既未经用户同意，也未做匿名化处理，通过客户端嵌入的 Crashlytics 等 SDK 将收集 Android ID 等个人信息传输到美国亚马逊云服务器。
3.	某互动 App	以默认选择同意隐私政策的非明示方式征求用户同意。
4.	某教育 App	既未经用户同意，也未做匿名化处理，向第三方提供用户的账号信息。
5.	某绘本 App	（1）以不正当方式误导用户同意收集儿童的头像和姓名等个人信息：以“会推荐更合适宝贝的绘本哦”为由收集儿童头像和姓名。 （2）征得用户同意前就开始收集应用程序列表等个人信息。
6.	某生活 App	用户撤销电话权限授权，明确表示不同意收集该权限对应的个人信息后，仍通过其他途径收集设备 IMEI 号等个人信息。

7.	某教育 App	未以显著方式展示隐私政策：注册或登录选项与同意隐私政策的因果逻辑关系不清楚。
8.	某借贷 App	App 关闭后，未经用户同意，采用自启动方式收集设备 IMEI 号等个人信息。
9.	某金融 App	手机开机后，未经用户同意，App 自启动并向第三方服务器发送数据。
10.	某游戏 App	将 targetSDKversion 值设置小于 23，要求用户一次性同意开启多个可收集个人信息的权限，用户不同意则无法使用。

针对公示通报的App，App违法违规收集使用个人信息治理工作组建议相关App运营者及时对存在的问题进行整改，工作组将对整改情况进行核验，并向相关部门提交复核结果，且将对不能有效整改的建议依法予以处置。如果企业拒不整改，可能受到基于《网络安全法》等法律法规的处罚，包括但不限于警告、没收违法所得、并处违法所得一倍以上十倍以下罚款（无违法所得的，处一百万元以下罚款）、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照等。此外，情节严重者如违法向他人出售或者提供公民个人信息，可能会进一步招致刑事责任。

二、与App中的同意相关的具体规则

《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》（以下简称**“《自评估指南》”**）等相关法律法规中规定了App收集使用个人信息的六个评估点，其中有两个评估点与用户同意密切相关，即“必须征得用户同意后才收集使用个人信息”和“经用户同意后才向他人提供个人信息”，其具体内容如下表所示，可供企业在合规管理中自评估参考使用。

基本规范	规范要点及具体要求
必须征得用户同意后才收集使用个人信息	• 收集个人信息或打开可收集个人信息权限前应当征得用户同意，且必须提供可由用户自主作出同意或不同意的选项。 • 用户明确表示不同意收集后不应以任何形式收集该类个人信息或打开该类可收集个人信息权限。 • 用户明确表示不同意收集后不应频繁征求用户同意、干扰用户正常使用，如在每次重新打开 App、或使用某一业务功能时，向用户频繁询问（**48 小时内询问超过一次**），但是用户主动选择使用的某一具体功能触发征得同意的动作不属于频繁干扰情形。 • 不应以默认选择同意隐私政策等非明示方式征求用户同意。如果通过设置“下一步”“注册”“登录即代表同意”等方式征求用户同意的情形，除以显著方式展示隐私政策等收集使用规则外，还需明确执行上述动作与同意隐私政策之间的逻辑关系，以达到主动提醒用户主动阅读隐私政策后征求用户同意的效果。 • 未经用户同意，不应更改其设置的可收集个人信息权限状态。 • 不应以不正当方式误导用户同意收集个人信息，不应故意欺瞒、掩饰收集使用个人信息的真实目的，不得诱骗用户同意收集个人信息或打开可收集个人信息权限（例如 App 提示用户打开通讯录权限以参与红包、金币、抽奖等活动）。 • 应当向用户提供撤回同意收集个人信息的途径、方式。如用户拒绝或关闭可收集个人信息权限时，不应影响用户正常使用与该权限无关的业务功能，不应暂停其他业务功能，或降低其他业务功能的服务质量。 • 开展个人信息处理活动需严格遵循所公开的隐私政策等收集使用规则，并遵守与用户的约定；如个人信息使用目的、方式、范围等发生变化的，需再次征得用户同意。
经用户同意后才向他人提供个人信	1.向他人提供个人信息前应当征得用户同意 • 如存在从客户端直接向第三方发送个人信息的情形，包括通过客户端嵌入第三方代码、插件（如 SDK）等方式向第三方发送个人信息的情形，需事先征得用户同意，经匿名化处理的除外。

息		• 如个人信息传输至服务器后，App 运营者向第三方提供其收集的个人信息，需事先征得用户同意，经匿名化处理的除外。 • 如向第三方传输的个人信息类型、接收数据的第三方身份等发生变更的，需以适当方式通知用户，并征得用户同意。
	2.向接入的第三方应用提供个人信息前应当经用户同意	• 如 App 接入第三方应用，当用户使用第三方应用时，需在征得用户同意后，再向第三方应用提供个人信息；当用户获知应用为第三方提供后，自行以主动填写等方式向第三方直接授权的除外。

三、特殊领域的同意规则

对待某些特殊群体或者处理某些特殊信息时，出于对这些人群和信息的额外保护，相关法律法规中上对于收集使用这些特殊领域的信息规定了一些针对性的告知同意规则。以下简要介绍分析法律法规中对于儿童或未成年人、生物识别信息、个人敏感信息这三个特殊领域的告知同意规则。

（一）儿童或未成年人

儿童或未成年人属于一类特殊群体，收集使用其信息时需要付诸格外的关注。

首先，根据《儿童个人信息网络保护规定》，网络运营者收集、存储、使用、转移、披露儿童个人信息的，应当遵循正当必要、知情同意、目的明确、安全保障、依法利用的原则。网络运营者收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的同意。网络运营者使用儿童个人信息，不得违反法律、行政法规的规定和双方约定的目的、范围。因业务需要，确需超出约定的目的、范围使用的，应当再次征得儿童监护人的同意。网络运营者征得同意时，应当同时提供拒绝选项，并明确告知以下事项（如果告知事项发生实质性变化的，应当再次征得儿童监护人的同意）：

a) 收集、存储、使用、转移、披露儿童个人信息的目的、方式和范围；

b) 儿童个人信息存储的地点、期限和到期后的处理方式；

c) 儿童个人信息的安全保障措施；

d) 拒绝的后果；

e) 投诉、举报的渠道和方式；

f) 更正、删除儿童个人信息的途径和方法；

g) 其他应当告知的事项。

此外，儿童或者其监护人要求网络运营者删除其收集、存储、使用、披露的儿童个人信息的，网络运营者应当及时采取措施予以删除，包括但不限于以下情形：

a) 网络运营者违反法律、行政法规的规定或者双方的约定收集、存储、使用、转移、披露儿童个人信息的；

b) 超出目的范围或者必要期限收集、存储、使用、转移、披露儿童个人信息的；

c) 儿童监护人撤回同意的；

d) 儿童或者其监护人通过注销等方式终止使用产品或者服务的。

其次，根据《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》”**），收集年满14周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满14周岁的，应征得其监护人的明示同意。同时根据《信息安全技术 个人信息告知同意指南》（以下简称**“《告知同意指南》”**），除了上述规定之外，同时还应当将个人信息使用规则等信息告知该未成年人或其监护人。根据《告知同意指南》，个人信息控制者在收集使用未成年人信息时应当额外告知以下内容：

a) 未成年人个人信息的敏感性与注意事项；

b) 针对未成年人个人信息的敏感性所采取的特别的安全保障措施；

c) 监护人更正、管理未成年人个人信息的方式和途径；

d) 监护人正确履行监护职责，教育引导儿童增强个人信息保护意识和能力的方式；

e) 若涉及幼儿园、学校等决定采用自动化设备收集未成年人个人信息的，可以说明采取此类措施的正当性、合法性与必要性，有必要时可提供相关的个人信息安全影响评估报告的全文或摘要，与监护人进行集体沟通的，可以告知沟通的总体情况与结论。

另外，根据欧盟的《一般数据保护条例》（以下简称**“GDPR”**）的规定，在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的情况下，对于为儿童直接提供信息社会服务的请求，当儿童年满16周岁，对儿童个人数据的处理是合法的。当儿童不满16周岁，只有当对儿童具有父母监护责任的主体同意或授权，此类处理才是合法的。控制者应当采取合理的努力，结合技术可行性，确保此类情形中对儿童具有父母监护责任的主体已经授权或同意。需要注意的是，针对是否需要获取监护人同意的年龄界限，GDPR中的年龄较中国法中的年龄更高，中国为14周岁，而欧盟为16周岁，如果企业收集处理儿童的个人信息时可能适用GDPR，那么应当格外关注年龄界限的差异。

（二）生物识别信息

个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。根据《个人信息安全规范》，收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。同时，个人生物识别信息原则上不应共享、转让。因业务需要，确需共享、转让的，应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。

（三）个人敏感信息

根据《个人信息安全规范》，收集个人敏感信息前，应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示。加工处理而产生的个人信息属于个人敏感信息的，对其处理需符合对个人敏感信息的要求。共享、转让个人敏感信息前，除向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果，并事先征得个人信息主体的授权同意（共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别或者关联个人信息主体的除外）之外，还应向个人信息主体告知涉及的个人敏感信息类型、数据接收方的身份和数据安全能力，并事先征得个人信息主体的明示同意。

同时，根据《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》，相较前述规定，进一步强调涉及个人敏感信息的，应当逐项征得个人信息主体的明示同意。

四、相关罚则

参考国际相关规定，根据GDPR第83条，违反处理的基本原则，包括第5、6、7和9条规定的同意的条件，应当按第2段的规定施加最高20,000,000欧元的行政罚款，如果是企业的话，最高可处相当于其上一年全球总营业额4%的金额的罚款，两者取其高的一项进行罚款。

而在国内，根据《网络安全法》第六十四条的规定，网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款[1]、第四十一条至第四十三条[2]规定，侵害个人信息依法得到保护的权利的，由

[1] 网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

[2] 《网络安全法》第四十一条：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。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

《网络安全法》第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的

有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

此外，违法收集使用个人信息也可能触犯刑法而进一步涉及刑事责任的追究。根据《中华人民共和国刑法》第二百五十三条之一（侵犯公民个人信息罪），违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

五、合规建议

综上所述，企业在收集使用个人信息时，应当严格遵循《网络安全法》、《个人信息安全规范》、《告知同意指南》、《自评估指南》、《儿童个人信息网络保护规定》等法律法规中关于告知同意规则的要求，避免在这方面违规而招致行政责任甚至刑事责任。此外，出于证据留存和合规要求，企业应当按照如下要求留存告知同意的证据：

a) 应当留存个人信息主体初次选择同意特定个人信息处理活动以及后续变更或撤回同意的证据；

b) 告知同意证据内容主要包括：时间，事项，目的等，针对可能产生高风险的个人信息收集行为，还需留存具体的告知同意；

c) 可以根据自身情况灵活选择证据留存的方式。例如，在网络环境中，可以留存当时个人信息主体授权同意的页面、告知同意的工作流程、个人信息主体同意行为的记录（如日志）以及提供给个人信息主体的告知内容；

d) 只要有关的个人信息处理活动持续存在，企业证明告知同意的义务就持续存在；在处理活动结束后，证据留存不应超过履行法律义务、提起或应对诉讼、纠纷的必要限度，例如以诉讼时效为限；

e) 对于授权同意证据的留存，需避免因证据留存导致产生收集额外个人信息的情形。

同时，根据《告知同意指南》，在不同场景下收集个人信息有不同的要求，例如SDK收集使用个人信息场景、物联网loT场景、公共场合场景、个性化推荐场景、互联网金融场景、车载场景、网上购物场景等，企业可根据自身的经营情况参见该指南附录或咨询相关专业机构。

情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

《网络安全法》第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

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