《信息安全技术 个人信息处理中告知和同意的实施指南》——构建“告知 – 同意”体系

敏于知

背景

《个人信息保护法》的发布，初步构建了“告知 – 同意”的个人信息处理规则和个人信息处理的一种合法性基础，但个人信息处理者在实践中对于告知与同意的具体操作标准尚存疑问。例如，企业按照《个人信息保护法》要求，处理敏感个人信息时应获取个人的“单独同意”，但在实际操作过程中，企业发现很难定义实施“单独同意”的表现形式（单独制定处理敏感个人信息隐私政策并要求获取个人同意，或在现有隐私政策中突出显示关于处理敏感个人信息的个人信息处理规则）。与此同时，处理规则告知不清晰，一揽子同意等现象时有发生。

2023 年 5 月 23 日，国家标准化管理委员会和国家市场监督管理总局联合发布了国标 GB/T 42574–2023《信息安全技术 个人信息处理中告知和同意的实施指南》（《Information security technology — Implementation guidelines for notices and consent in personal information processing》）（以下简称《指南》），将于 2023 年 12 月 1 日正式生效。《指南》对告知与同意的适用情形、告知和同意的基本原则、告知的方式、内容和实施，以及同意机制的选择、实施、撤回和证据留存等进行了细致的规定，并通过附录详细列举了不同场景下的告知和同意。

告知与同意的适用情形

《个人信息保护法》第十七条中规定个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知相关事项。《指南》对收集、提供、公开个人信息、处理活动发生变更等处理个人信息的情形分别进行阐述，并结合实践具体说明需要进行告知、同意的场景（详见表一）。

表一：“告知 – 同意”适用情形及场景

告知同意情形	具体场景
收集个人信息	• 个人填写勾选上传 • 系统自动采集（包括 SDK、API、浏览器、智能终端、传感器、摄像头等） • 交互行为记录（记录个人浏览、交易、客服咨询、使用服务等） • 从第三方间接获取 • 从非完全公开渠道获取 • 从与个人相关的他人账号收集 • 使用技术分析关联或生成
提供、公开个人信息	• 向其他个人信息处理者提供 • 向境外提供 • 在一定范围内或向不特定范围公开 • 因合并、分立、解散、被宣告破产等原因转移

处理活动等发生变更	• 处理目的、处理方式、个人信息种类、公开范围发生变更 • 接收方处理目的、处理方式、名称或者姓名和联系方式发生变更 • 保存期限延长 * • 个人信息处理者的名称或者姓名和联系方式发生变更 * • 个人行使其权利的方式和程序发生变更 *
其他情形	• 两个及以上的个人信息处理者共同决定个人信息的处理目的和处理方式 • 在产品或服务中接入需处理个人信息的其他个人信息处理者的产品或服务 • 处理的个人信息涉及该个人以外的其他人 • 处理已公开的个人信息，对个人权益有重大影响 • 停止运营某类业务功能，或停止运营产品或服务时 * • 个人行使权利，可能对其权益产生影响 * • 发生或者可能发生个人信息泄露、篡改、丢失等安全事件时 * • 以下情形中处理个人信息的，采取适当方式向个人进行告知：* – 为订立、履行个人作为一方当事人的合同所必需，或者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 – 履行法定职责或者法定义务所必需 – 为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需 – 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息 – 在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息 – 法律法规规定的其他情形

注：* 为需要向个人告知但免于获取同意的场景，其余场景均需获取个人同意。

告知

个人信息处理者在实施告知时需考虑以下基本原则：

- **公开透明：**公布处理个人信息的种类、目的、方式、安全措施等处理规则，不采取故意遮挡、隐藏等方式诱导个人略过告知内容；
- **有效传达：**尽可能通过交互式界面、邮件、电话或短信等方式向相关个人进行告知；
- **适时充分：**在收集、提供、公开等个人信息处理活动发生之前或同时，对个人进行充分告知；真实明确：告知个人信息的处理种类、目的、方式等规则与实际情况一致，且需结合实际业务功能，不使用笼统、宽泛的表述；
- **清晰易懂：**告知文本符合个人的语言习惯，使用通用且无歧义的语言、数字、图示等。

1. 告知方式

《指南》将告知的方式明确分为三类：一般告知、增强告知和即时提示。个人信息处理者需根据产品或服务特点、想要达到的告知目的、监管要求等，采用最为恰当的告知方式（下图一介绍了三种告知方式的主要应用情形及形式）。

图一：告知方式对比

一般告知	增强告知	即时提示
主要用于个人信息处理者在处理个人信息前向个人全面阐述个人信息处理规则，且通常采用制定、展示个人信息保护政策（或被称为“隐私协议”“隐私政策”“隐私权政策”等）的形式进行告知。	主要用于帮助个人理解个人信息处理规则中的关键内容或与特定业务功能处理目的相关的个人信息处理规则，且通常采用个人不可绕过的方式（如设置专门界面或单独步骤）向个人告知相关信息，以协助个人作出是否同意的决定。	主要用于在个人使用产品或服务过程中，进一步强化个人对收集个人信息的目的的理解、方便个人获取有价值的信息。
应用情形 • 首次收集个人信息 • 为满足不同业务功能特点、不同收集个人信息方式告知的具体需求	**应用情形** • 在产品或服务的基本业务功能开启前（如个人初始安装、首次使用、注册账号等情形） • 在个人选择使用扩展业务功能或新增业务功能时 • 涉及开通收集个人生物识别信息的业务功能，或某业务功能处理个人生物识别信息前 • 涉及通过间接方式获取个人信息的 • 产品或服务涉及收集不满 14 周岁的未成年人个人信息的 • 涉及首次提供、主动跨境、公开、转移个人信息 • 涉及软硬件自动采集信息 • 因产品或服务处理个人信息活动发生变更、更新个人信息保护政策 • 产品服务停止运营 • 个人注销账号 • 个人信息安全事件等 • 需要取得单独同意的情况	**应用情形** • 在收集个人信息的过程中，需个人予以配合的（如人脸识别时需要个人点头配合） • 业务功能可能导致其个人信息被公开的（如群组内发言、发布信息、回复评论、参加抽奖评选活动、接受访谈或个人信息被用于宣传推广） • 因产品或服务处理个人信息活动发生变更，更新个人信息保护政策（不涉及重新取得同意的政策更新） • 个人使用涉及其他个人信息处理者的业务功能 • 处理个人信息涉及个人以外的其他人 • 个人行使权力 • 涉及《个人信息保护法》第十三条规定的免于个人信息同意时，如需要个人必须主动提供个人信息的 • 个人行为可能导致个人信息风险 • 个人询问、投诉等 • 通过分析投诉、举报信息、社会反映情况等方式得知个人对某些个人信息处理规则不明，进一步解释说明 • 其他与个人权益密切相关、需要向个人强调的信息
主要形式 • 完整内容置于产品或服务的基本业务功能开启时与告知相关的交互式界面中，并通过弹窗提示、提醒勾选、突出链接等明显方式，主动提示个人阅读个人信息保护政策 • 无法实现交互式界面展示时，以其他方式且在收集个人信息前的必要环节，以发送通知、邮件（或信件）、提供文档（包括电子版或纸质版）、张贴告示、 播放音视频等方式向个人主动提供或展示 • 无法逐一告知时，可通过公告的形式发布个人信息保护政策	**主要形式** • 采用个人不可绕过的方式（如设置专门界面或单独步骤） • 凸显与一般告知方式的差异，采用弹窗等方式向个人直接展示或送达关键内容 • 涉及产品、服务、业务停止运营等特殊情况，通过邮件、短信、站内信等可保证个人可**随时查阅**的告知方式 • 涉及可能对个人权益产生重大影响的个人信息处理活动时，可选择使用电话、语音提示等**确保送达**的方式	**主要形式** • 使用弹窗、 浮窗或浮层、文字说明、状态栏提示、提示条或提示框、提示音、短消息等方式

在告知实施中，《指南》也通过收集个人信息、提供和公开个人信息、处理活动发生变更，及其他情形介绍了各场景下的告知形式及内容，下图的“告知示例”以收集个人信息时为例，展示了三种不同的告知形式。

例：一般告知（首次收集个人信息）

例：增强告知（收集位置等敏感个人信息，告知处理个人信息的目的、处理的必要性和对个人权益的影响）

例：即时提示（更新个人信息保护政策）

2. 告知时机

大多数企业往往认为告知仅需发生在产品或服务开始收集个人信息前，如账户注册阶段，但事实上在许多场景下需要企业再次告知相关个人信息处理规则。为提高告知的充分性及有效性，帮助《指南》将告知的时机分为首次告知、同步告知和再次告知三类，企业可以参考下方表二的告知时机对照表，并以适当的频率平衡用户体验和告知要求，对个人信息主体进行告知。

表二：告知时机对照表

告知类型	告知场景
首次告知	• 个人在首次使用产品或服务前
同步告知	• 如业务功能需不间断或反复多次向其他个人信息处理者提供个人信息（首次提供时同步告知，并说明后续提供的时机或频次等规则） • 在收集个人信息时，对个人权益影响较大、收集的必要性需要单独强调、相关业务功能收集目的不易理解的 • 如业务功能所收集个人信息的必要性较为直接易懂、个人通常无需被另行告知即可理解的（告知业务功能名称视为处理目的） • 通过其他载体收集或间接获取个人信息时 • 向其他个人信息处理者提供个人信息前 • 个人注销账户时 • 停止业务功能运营前 • 发生对个人信息有严重影响的安全事件时
再次告知	• 变更个人信息处理目的、方式、范围前 • 通过其他载体收集或间接获取个人信息时，因客观条件所限，如无联系渠道（获取个人信息后再次告知） • 个人拒绝对收集、提供、变更目的等的请求（再次告知必要性和对个人权益的影响） • 产品或服务更新后个人信息保护政策发生变化的

同意

个人信息处理者在取得个人同意时需考虑以下基本原则：

- **告知一致：**取得同意的范围不超出所告知的内容；
- **自主选择：**支持个人通过自行操作的方式作出同意，不使用默认勾选的方式取得同意；
- **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，取得个人同意，以增进个人对业务功能与所收集的个人信息之间关联性的理解；
- **避免捆绑：**区分产品或服务的业务功能，不采用捆绑方式强迫个人一次性同意多种业务功能可能收集的个人信息或多个处理活动；个人拒绝同意时，不影响与该个人信息无关的业务功能的正常使用。

1. 同意的实施

《指南》明确了不同同意机制的适用场景及实施要点，为企业在进行个人信息处理活动时提供了指引。对于需要取得个人同意的个人信息处理活动，原则上需使用明示同意的方式，而某些特定场景下，根据法律法规要求，企业可参考下表三选择实施单独同意或书面同意的机制。

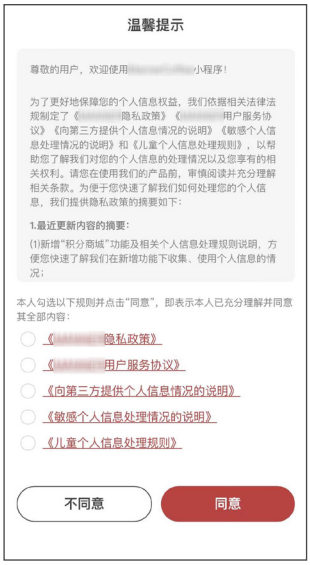
表三：同意实施机制

	适用场景	实施重点
明示同意	• 需要取得同意的个人信息处理活动	明示同意的方式较为直接，包括但不限于： • 个人通过交互式界面作出主动勾选、主动点击“同意”“下一步”“继续”、滑动滑块、主动发送等动作表示意愿 • 个人通过主动填写、上传、输入个人信息表示意愿 • 个人通过开启可收集个人信息的 API、权限、传感器开关表示意愿 • 个人通过纸质或电子的书面声明、签字确认表示意愿（注：该方式通常被用于表示书面同意） • 个人通过主动出示证件、刷卡、刷指纹、刷脸等动作表示意愿 • 个人通过回复邮件、短信息等主动联络的方式表示意愿 • 个人通过电子签名方式表示意愿 • 个人通过电话录音、视频录像等方式表示意愿
推定同意	在**同时满足以下四个条件**的情况下，如因实际原因无法表达明示同意，基于对个人行为的分析，如个人未明确表示拒绝个人信息处理，或个人选择继续使用特定业务功能时，可以推定认为个人表示同意： • 取得明示同意存在显著困难 • 经个人信息保护影响评估确认个人信息的处理不会对个人权益造成不利影响 • 采取了适当的方式向个人告知了个人信息处理规则 • 被推定为个人同意的情形不影响个人行使撤回同意的权利	• 在后续的个人信息处理活动中，如个人信息处理者具备执行明示同意的条件时，需向个人告知撤回同意的方式，或重新取得个人的明示同意 • 如个人通过投诉、举报渠道反馈其个人权益受到不利影响的，经确认后需立即中止相关的个人信息处理活动，经个人明示同意的处理活动除外

单独同意	• 向其他个人信息处理者提供个人信息 • 公开个人信息 • 将在公共场所通过图像采集、个人身份识别设备所收集的个人图像、身份识别信息用于维护公共安全之外的目的 • 处理敏感个人信息 • 向境外提供个人信息 • 评估后认为可能对个人权益带来重大影响的个人信息处理活动（《指南》新增）	• 需选择明示同意的方式来取得个人单独同意 • 单独同意所针对的个人信息处理活动应为具体而独立的目的或业务功能，在个人作出单独同意之前，个人信息处理者还应当通过**增强告知**的方式告知需要单独同意的情形 • 如特定业务功能为产品或服务的基本业务功能，可将需单独同意的情形相关告知内容以**突出显示、弹窗等与其他内容有所区分的方式单独告知**，在个人同意使用基本业务功能时一并同意 • 单独同意为个人针对其个人信息进行特定处理而专门作出具体、明确授权的行为，不包括一次性针对多种目的或方式的个人信息处理活动作出的同意，即不得要求个人概括同意
书面同意	• 在广告中使用他人名义或者形象 • 通过指定网络通道送达某些类型的诉讼文书 • 采集人类遗传资源 • 征信机构采集个人的收入、存款、有价证券、商业保险、不动产的信息和纳税数额信息 • 向征信机构查询个人信息 • 使用金融信用信息基础数据库查询个人信息 • 从事信贷业务功能的机构向金融信用信息基础数据库或者其他主体提供信贷信息等 • 邮政企业、快递企业及其从业人员向他人提供用户的个人身份信息及其使用邮政服务、快递业务功能的信息 • 为宣传报道和奖励检举有功人员而公开检举人的相关个人信息 • 用人单位公开劳动者的个人信息 • 商业银行与合作机构共享客户个人信息 • 受托人转委托其他个人信息处理者处理个人信息	• 在个人作出书面同意之前，需通过**增强告知且以书面形式呈现**的机制，针对需要书面同意的内容明确向个人进行充分告知 • 需选择**明示同意**的机制取得个人的书面同意，且明示同意需以**文字形式**予以明确表达，不以采取个人点击确认、点击同意、上传提交、登录使用或配合拍照等表示同意的方式取得个人的书面同意 • 选择易于展示、便于操作的书面同意具体实施方案，例如，个人在纸质界面、电子硬件载体、网页交互式界面或对话框上进行手写签名、签章等 • 如根据法律法规等要求，个人信息处理者既需要取得个人书面同意也需要取得其单独同意的，需在书面同意的基础上，设计单独同意的机制，如单独签名、签章等

除《个人信息保护法》要求采取单独同意的情形外，此次《指南》中新增的“评估后认为可能对个人权益带来重大影响的个人信息处理活动”，也应取得个人单独同意，如实施对个人信用、绩效评定、所接受服务的质量、交易价格等会对自然人人格尊严、人身或财产安全等产生重大直接影响的自动化决策等活动。下图的“单独同意示例”呈现了部分单独同意实现机制，企业可参考《指南》附录中的示例业务场景，并根据自身产品服务设计其告知及同意机制。

分项勾选同意多个需要单独同意的情形



特定业务功能单独交互式页面

弹窗获取处理敏感个人信息的单独同意

2. 拒绝同意及撤回同意

个人可通过点击拒绝、中断操作、关闭界面、回退到上一步等操作进行拒绝或放弃同意，个人信息处理者需明确以上拒绝同意的表现形式，在个人未完成同意操作前，避免收集在个人同意过程中涉及的个人信息。

- 个人拒绝同意后，宜采用适当的方式向个人展示、说明拒绝后的后果，不以频繁询问、请求同意方式对个人造成打扰（个人信息为服务所必须的除外）；
- 个人拒绝某业务功能处理个人信息后，不宜退出产品或服务的所有界面，宜保持原有界面，或切换至产品或服务的基本业务功能或其他相关业务功能的界面；
- 个人拒绝同意产品或服务的基本业务功能处理个人信息后，可切换至不涉及个人信息处理的服务模式（如静态页面、非个性化的浏览页面等）。

《指南》要求个人信息处理者明确撤回同意的操作（如交互式功能页面、电话、邮箱等方式），并可通过一般告知的方式，在个人信息保护政策中向个人说明撤回同意的具体场景和操作方法。撤回同意的颗粒度需根据个人实际需求和产品服务特点设计，撤回某个业务的个人信息处理同意的，不得拒绝提供其他业务功能或降低其他业务质量（除非撤回同意的个人信息是其他业务功能所必需）。

个人撤回同意后，应设计并向个人主动告知删除或匿名化相关个人信息的机制，以供个人作出是否保留个人信息的选择；个人信息处理者后续不得再处理相应的个人信息，但不影响撤回前基于个人同意已进行的个人信息处理活动的效力；个人信息处理者需在承诺时限内（不超过 15 日）完成对撤回同意请求的确认，以及完成删除或匿名化相关个人信息的操作，并向个人反馈撤回同意的结果。

结语

此次出台的《指南》是倾向于实务操作的指南性文件，旨在为个人信息处理者在面对各种情形时提供具体的实务建议。除了上述内容，《指南》还提供了数十种实践场景下的的告知和同意机制的实施要点和建议，包含 App 基本业务功能与拓展业务功能、App 嵌入第三方 SDK 场景、处理不满 14 周岁未成年人、智慧生活场景、公共场所场景、个性化推送场景、云计算服务场景、车内场景、互联网金融场景、网上购物场景、快递物流场景、互联网房产经纪服务场景、个人身份认证场景的告知和同意，帮助企业更好地适应以“告知 — 同意”为核心的个人信息处理规则，企业可以结合自身业务场景取而用之。

达于行

甫瀚咨询可提供的服务

甫瀚咨询为企业提供企业数据安全风险评估，帮助企业提升数据安全治理水平，并根据国家最新数据安全及隐私相关法规，协助企业降低在数据及隐私处理活动中的合规风险，为优化企业综合安全治理水平奠定基础。我们可提供的数据安全相关服务包括：

个人信息安全风险评估

梳理客户个人信息资产，基于法律法规要求及行业最佳实践，从个人信息保护治理到全生命周期评估安全风险。

数据安全风险合规评估

保护客户最珍贵的数据资产，在企业数据安全管理和运营的基础上，为数据的全生命周期进行定制化的安全评估。

数据跨境安全风险评估

进一步确定出境数据的类型以及对应风险，对企业组织保障与技术保障进行检查，在保障数据安全的基础上促进数据流动。

个人信息保护影响评估

在对应场景中，超越“静态底线式”的个人信息保护合规，有效、全面地掌握信息处理行为对个人合法权益影响的风险变化，有针对性地提出安全保护措施，达到动态优化权益保护效果，以适应风险态势的变化。

安全意识及能力培训

针对行业 / 企业 / 部门 / 角色等高度定制化的安全意识与能力培训，提供最大化的效率和安全意识，确保人员管理不再是企业安全的短板。

关于甫瀚咨询

甫瀚咨询是一家全球性的咨询机构，为企业带来领先的专业知识、客观的见解、量身定制的方案和卓越的合作体验，协助企业领导者们充满信心地面对未来。透过甫瀚咨询网络和遍布全球超过25个国家的逾85家分支机构和成员公司，我们为客户提供财务、信息技术、运营、数据、数字化、环境、社会及管治、治理、风险管理以及内部审计领域的咨询解决方案。

甫瀚咨询荣膺2023年《财富》杂志年度最佳雇主百强，我们为超过80%的财富100强及近80%的财富500强企业提供咨询服务，亦与政府机构和成长型中小企业开展合作，其中包括计划上市的企业。甫瀚咨询是Robert Half International Inc.（纽约证券交易所代码：RHI）的全资子公司。RHI于1948年成立，为标准普尔500指数的成员公司。

联系我们

余达丽
项目总监
Angela.Yu@protiviti.com

尹必成
高级咨询顾问
Oliver.Yin@protiviti.com

公司地址

北京
朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话：(86.10) 8515 1233

上海
徐汇区陕西南路 288 号
环贸广场二期 1915-16 室
电话：(86.21) 5153 6900

深圳
福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话：(86.755) 2598 2086

香港
中环 干诺道中 41 号
盈置大厦 9 楼
电话：(852) 2238 0499

protiviti 甫瀚