

敏感个人信息单独同意的规范构造

以同意的有效性、独立性及其界限为中心

赵跃

(安徽国运律师事务所, 安徽 合肥 230000)

摘要: 个人信息保护法第二十九条对敏感个人信息的处理设置了“单独同意”规则, 其规范目的在于提高同意的门槛, 使信息主体在处理其生物识别、医疗健康、金融账户、行踪轨迹等信息时, 获得更为充分的告知与更为真实的选择。但“单独”的含义、同意的有效性、撤回的后果、以及与第二十三条、第二十五条、第二十六条的关系, 实务中理解不一。本文主张, “单独”具有三重含义: 其一, 独立于其他处理事项, 即不得以概括同意替代; 其二, 独立于其他条款, 即不得与服务协议捆绑; 其三, 独立的意思表示, 即须有可识别的、可回溯的同意行为。单独同意的有效性, 须具备自愿、明确、知情、具体四项要件, 其中“具体”要求告知处理目的、方式、种类、保存期限与必要性。撤回同意是信息主体的法定权利, 撤回后处理者应当停止处理, 但不得因此拒绝提供与处理目的无关的服务; 若处理系提供服务所必需, 则拒绝服务具有正当性。例外情形包括: 履行法定义务、应对突发公共卫生事件、为履行合同所必需等, 此时无须取得单独同意, 但仍须履行告知义务。举证责任上, 处理者应当就同意的取得、内容与范围承担证明责任; 未能证明的, 视为未取得同意。合规路径上, 应当建立单独的告知界面、独立的勾选机制、可撤回的技术设计, 以及事前影响评估的记录。

关键词: 敏感个人信息; 单独同意; 知情同意; 撤回同意; 影响评估; 举证责任

中图分类号: D923.1 **文献标识码:** A **文稿编号:** WJLT(2025)05-0040-14

The Normative Construction of Separate Consent for Sensitive Personal Information: Validity, Independence, and Limits

ZHAO Yue

(Anhui Guoyun Law Firm, Hefei 230000, Anhui, China)

Abstract: Article 29 of the Personal Information Protection Law establishes a rule of separate consent for the processing of sensitive personal information, aiming to raise the threshold of consent so that data subjects obtain fuller disclosure and a more genuine choice when biometric, health, financial account, and location data are processed. Yet the meaning of "separate", the validity of consent, the consequences of withdrawal, and the relationship with Articles 23, 25, and 26 remain contested. This article argues that "separate" carries three meanings: independence from other processing items, independence from other contractual terms, and an identifiable expression of will. Valid separate consent requires voluntariness, explicitness, informedness, and specificity, the last demanding disclosure of purpose, method, categories, retention period, and necessity. Withdrawal is a statutory right; processing must cease upon withdrawal, though services unrelated to the processing purpose may not be refused. Exceptions include statutory duties, public health emergencies, and contractual necessity, where separate consent is not required but disclosure remains obligatory. The processor bears the burden of proving that consent was obtained, and failure to prove it amounts to absence of consent. Compliance requires separate disclosure interfaces, independent opt-in mechanisms, withdrawable technical design, and documented impact assessments.

Key words: sensitive personal information; separate consent; informed consent; withdrawal of consent; impact assessment; burden of proof

说明: (本文为作者个人研究观点, 不代表所在单位意见)

作者简介: 赵跃, 安徽国运律师事务所执业律师, 研究方向为民商法学、数据法学。

一、问题的提出

个人信息保护法第二十八条规定, 敏感个人信息是一旦泄露或者非法使用, 容易导致

自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

该条同时规定，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。第二十九条规定，处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

“单独同意”，是敏感个人信息处理的核心规则。其规范目的，在于提高同意的门槛：使信息主体在处理其最为私密的信息时，获得更为充分的告知，作出更为真实的选择。

但“单独”究竟何指？是“单独的界面”，还是“单独的勾选”，抑或“单独的合同条款”？实务中，处理者常以“一揽子同意”替代“单独同意”，以“继续使用即视为同意”替代“主动勾选”，以“隐私政策”替代“具体告知”。

监管执法中，此类做法屡被认定为违法。但认定的标准并不统一：有的执法机关要求“独立的弹窗”，有的要求“独立的勾选”，有的只要求“可识别的同意记录”。

学理上的讨论，也多集中于“告知同意”的一般原理，对“单独”这一修饰语的特殊含义，着墨不多。而恰恰是这一修饰语，构成了敏感个人信息保护的关键。

本文的基本主张是：“单独”具有三重含义，即独立于其他处理事项、独立于其他条款、独立的意思表示；单独同意的有效性，须具备自愿、明确、知情、具体四项要件；撤回同意是法定权利，撤回后不得拒绝与处理目的无关的服务；例外情形须严格把握；举证责任由处理者承担。

处理人脸、行踪、健康等信息为什么需要单独同意、如何判断是否合规，可参见“处理人脸、行踪、健康信息，要单独同意吗”一文的梳理；本文不重复合规清单，只讨论单独同意的教义构造与界限。

个人信息保护法的制定，标志着我国个人信息保护从“分散立法”走向“统一立法”。此前，相关规范散见于网络安全法、消费者权益保护法、民法典人格权编，其保护的水平和标准并不统一。

统一立法的核心，是“告知同意”规则。该规则的理据，在于“信息自决”：个人有权决定其信息是否被处理、如何被处理、由谁处理。

信息自决的理论，源自德国。其宪法法院在一九八三年的“人口普查案”中，确立了“信息自决权”，认为个人对其信息的披露与使用享有自我决定的权利。

我国虽未在宪法层面确认信息自决权，但民法典第一千零三十四条、第一千零三十五条，已将“同意”作为处理个人信息的基本规则。个人信息保护法进一步细化，形成了完整的规则体系。

须注意，同意不是“万能的”。即便取得同意，处理仍须遵守“合法、正当、必要”的原则；若处理违反法律的强制性规定，即便同意，也不能免责。

例如，处理法律禁止收集的信息（如基因信息用于就业歧视），即便取得同意，仍属违法。同意的功能，是“授权”，而非“豁免”。

比较法上，欧盟通用数据保护条例第九条对特殊类型数据（相当于我国的敏感个人信息）要求“明示同意”（明示同意），其标准高于一般同意。

我国采“单独同意”的表述，其含义与“明示同意”相近，但更强调“程序上的独立”：不仅是“明示”，还须“单独”。这一表述，更契合我国实务中“捆绑同意”泛滥的现状。

二、同意在个人信息处理中的定位

同意，是个人信息处理的合法性基础之一，但不是唯一的基础。个人信息保护法第十三条规定了六项基础：取得个人同意；为订立、履行合同所必需；为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；依照本法规定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。

六项基础之间，是并列关系，而非递进关系。处理者可以选择其中一项作为合法性基础；但一旦选择“同意”，便须遵守同意规则的全部要求。

同意的性质，学理上有“意思表示说”“授权说”“免责事由说”三种主张。意思表示说认为，同意是信息主体的法律行为，其效果是授权处理；授权说认为，同意是单方的授权行为，不构成合同；免责事由说认为，同意只是阻却违法的事由，不产生授权效果。

本文采“授权说”。理由在于：同意是单方行为，无须处理者承诺即生效；其效果是使本属违法的处理行为获得正当性；其内容是对特定处理行为的许可，而非对处理者的概括授权。

授权说的实益，在于解释同意的“范围性”：同意只在授权的范围内有效，超出范围的处理，仍属违法。这与“一揽子同意”的做法，形成鲜明对比。

须注意，同意与合同不同。合同的成立须有双方合意；同意只需信息主体单方作出。故处理者不能以“合同已成立”为由，主张信息主体必须同意。

同意与“告知”的关系，亦须明确。告知是同意的前提，同意是告知的结果；无告知则无同意，有告知未必有同意。二者不可混同。

实务中，处理者常以“已在隐私政策中告知”为由，主张已取得同意。此种主张，混淆了告知与同意：告知是“说明”，同意是“选择”；只有说明而无选择，不构成同意。

敏感个人信息的界定，是一个“场景化”的问题。同一信息，在不同场景下，其敏感性可能不同。例如，姓名在一般场景下不敏感，但在特定身份（如举报人）的场景下，则

可能高度敏感。

场景化的判断，须考虑三个因素：信息的性质、处理的场景、损害的可能性。三者结合，才能得出“是否敏感”的结论。

我国立法采“列举加兜底”的方式，其优点是明确，其缺点是不够灵活。为弥补这一缺点，须通过“等”字的解释，将新的信息类型纳入。

例如，基因信息。其一旦泄露，可能导致基因歧视，损害严重；虽未明文列举，但应纳入“等”的范围。

又如，声纹信息。其属于生物识别信息的一种，与指纹、人脸同类；虽未单独列举，但应归入“生物识别”。

再如，消费记录。其是否敏感，须结合场景判断：一般的消费记录不敏感；但涉及医疗、金融的消费记录，则可能敏感。

须注意，“特定身份”的表述，容易引起歧义。其含义，不是“特定的职业”，而是“一旦泄露可能导致歧视或者伤害的身份”，如宗教信仰、性取向、政治倾向、犯罪记录。

实务中，有的处理者将“特定身份”理解为“公职人员”“企业高管”，此种理解，偏离了立法的本意。

敏感性的判断，还须考虑“组合效应”。单一信息可能不敏感，但多项信息组合后，可能形成“画像”，从而具有敏感性。

例如，单独的位置信息不必然敏感，但与时间、消费记录组合，便可推断个人的生活规律、健康状况、社交关系，从而具有高度的敏感性。

三、敏感个人信息的界定

敏感个人信息的界定，采“概括加列举”的方式。概括部分，是“一旦泄露或者非法使用，容易导致人格尊严受到侵害或者人身、财产安全受到危害”；列举部分，是生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等。

概括部分的标准，是“损害的可能性与严重性”。可能性，指泄露或者非法使用后损害发生的概率；严重性，指损害后果的程度。二者结合，构成“敏感”的判断。

列举部分的功能，是“推定”：凡属列举范围的信息，推定为敏感；处理者若主张其不敏感，须承担证明责任。

“等”字的功能，是“兜底”：随着技术的发展，新的信息类型不断出现，如基因信息、声纹信息、步态信息，均可纳入“等”的范围。

须注意，敏感性与“匿名化”的关系。若信息经匿名化处理，无法识别特定自然人，则不再属于个人信息，自然也不属于敏感个人信息。但匿名化的标准甚高，实务中难以达到。

去标识化与匿名化不同。去标识化后的信息，仍可通过额外信息复原，故仍属个人信息；其处理，仍须遵守敏感个人信息的规则。

不满十四周岁未成年人的个人信息，一律视为敏感个人信息。这一规则的理据，在于未成年人的认知能力与自我保护能力不足，须给予特殊保护。

处理未成年人信息，须取得其父母或者其他监护人的同意，并制定专门的个人信息处理规则。此处的“同意”，是“单独同意”加“监护人同意”，双重门槛。

实务中，有的处理者以“用户勾选了‘我已满十四周岁’”为由，主张已尽审查义务。此种做法，不足以免责：处理者仍须采取合理措施，核实用户的年龄。

第二十九条的“单独”，与第二十三条、第二十五条、第二十六条的“单独同意”，在含义上应当一致。四条共同构成“单独同意”的规范群。

第二十三条规定，向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。

第二十五条规定，个人信息处理者公开其处理的个人信息的，应当取得个人单独同意。公开是“向不特定人披露”，其风险高于“向特定人提供”，故须单独同意。

第二十六条规定，在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识；所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

四条的关系，可以概括为：第二十九条是“一般规则”，第二十三条、第二十五条、第二十六条是“特别场景”。特别的场景，须同时满足一般规则与特别规则。

实务中，有的处理者只满足特别规则，而忽略一般规则。例如，在公共场所采集人脸，设置了提示标识，但未取得单独同意。此种做法，仍属违法。

“单独”的程序设计，可以有多种形式：独立的弹窗、独立的页面、独立的勾选框、独立的签名。形式可以多样，但实质须一致：可识别、可回溯、可选择。

可识别，是指同意的主体可以识别。若无法确认“是谁同意”，则同意不成立。故处理者应当记录同意的账号、时间、内容。

可回溯，是指同意的过程可以重现。若发生争议，处理者应当能够提供同意的界面截图、操作日志、版本记录。

可选择，是指信息主体可以选择“同意”或者“不同意”，且选择的后果不同。若两个选项的效果相同，则选择便是虚设。

四、“单独”的三重含义

“单独”的第一重含义，是独立于其他处理事项。即：处理敏感个人信息，须就该事项单独取得同意，不得将其纳入“概括同意”之中。

例如，某应用在隐私政策中列明“为提供服务，我们将收集您的位置信息、通讯录、人脸信息”，用户点击“同意”即视为同意全部。此种做法，不符合“单独同意”的要求。

正确的做法是：就每一项敏感个人信息处理，设置独立的告知与独立的勾选；用户可以选择同意其中一项，而拒绝另一项。

“单独”的第二重含义，是独立于其他条款。即：同意不得与服务协议、隐私政策中的其他条款捆绑，不得以“不同意即不能使用”相要挟。

个人信息保护法第十六条规定，个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，但是处理个人信息属于提供产品或者服务所必需的除外。

该条的规范意旨，在于防止“捆绑同意”：处理者不得以服务为筹码，迫使用户同意非必要的处理。对于敏感个人信息，这一要求更为严格。

“单独”的第三重含义，是独立的意思表示。即：同意须有可识别的、可回溯的行为，如主动勾选、单独点击、书面签署；不得以“继续使用即视为同意”推定。

沉默不构成同意。个人信息保护法第十四条规定，同意应当由个人在充分知情的前提下自愿、明确作出。“明确”二字，排除了默示同意的可能。

实务中，有的应用以“滑动页面即视为阅读并同意”作为同意方式。此种做法，不构成“明确”的意思表示，不符合法律的要求。

三重含义之间，是递进关系：独立于事项，是“范围”的要求；独立于条款，是“自愿”的要求；独立的意思表示，是“形式”的要求。三者兼备，方为“单独”。

知情同意的规则，最早形成于医疗领域。医生在实施手术前，须向患者说明风险，并取得其同意；未尽说明义务的，构成侵权。

个人信息领域的知情同意，借鉴了医疗领域的经验，但有其特殊性：医疗的同意是“一次性的”，个人信息的同意是“持续性的”；医疗的同意是“面对面的”，个人信息的同意是“线上的”。

持续性的特点，要求同意须“动态”：随着处理目的、方式的变化，同意应当更新；不能以“一次同意”覆盖“终身处理”。

线上的特点，要求同意须“可视化”：界面的设计、文字的表述、选项的设置，都影响同意的有效性。

实务中，有的处理者以“长达数十页的隐私政策”履行告知义务。此种做法，形式上合规，实质上无效：多数用户不会阅读，即便阅读也难以理解。

较为可取的做法是“分层告知”：第一层，以简明的语言说明核心内容（收集什么、用来做什么、保存多久）；第二层，以详细的条款说明具体规则；第三层，提供全文供查阅。

分层告知的优点，在于兼顾“可理解”与“完整性”：用户可以在短时间内了解核心内容，也可以在需要时查阅详细条款。

“具体”的要求，还意味着同意须“目的特定”。若处理目的表述为“提升服务”“优化体验”，则过于抽象，不符合“特定”的要求。

目的特定的实益，在于“目的限制”：处理者只能在同意的目的范围内处理；超出范围的处理，须重新取得同意。

实务中，有的处理者在隐私政策中写入“以及其他合理用途”的兜底条款，试图扩大处理范围。此种条款，因违反“目的特定”，应当认定为无效。

五、单独同意的有效性要件

同意的有效性，须具备四项要件：自愿、明确、知情、具体。四项要件，缺一不可。

“自愿”，是指同意须出于信息主体的自由意志，不受欺诈、胁迫或者不当影响。若处理者以“不授权即退出”相威胁，则同意不自愿。

判断自愿的标准，是“有无合理的选择空间”。若信息主体除了同意别无选择，则其同意难谓自愿；但若处理系服务所必需，则“不同意即不能使用”具有正当性。

“明确”，是指同意须以清晰的方式作出。模糊的表述、含糊的措辞、隐蔽的勾选，均不符合“明确”的要求。

实务中，有的处理者将“同意”选项预设为勾选状态，用户须主动取消。此种“默认同意”，不符合“明确”的要求。

“知情”，是指信息主体须在充分了解处理的目的、方式、种类、范围、保存期限、以及其权利的情况下作出同意。

个人信息保护法第十七条规定了告知的内容；第三十条规定，处理敏感个人信息的，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响。

“必要性”的告知，是敏感个人信息处理的特殊要求。其内容包括：为何必须处理该信息；不处理将产生何种后果；有无替代方案。

“影响”的告知，包括积极影响与消极影响。消极影响，如信息泄露的风险、被用于营销的可能、对个人评价的影响。

“具体”，是指同意须指向特定的处理行为，而非概括的授权。同意的内容，应当包括：处理的目的、方式、信息的种类、保存的期限、共享的对象。

四项要件中，“具体”最易被忽视。实务中，处理者常以“为提升服务体验”概括处理目的，此种表述过于抽象，不符合“具体”的要求。

撤回同意的制度价值，在于“纠正”：信息主体在同意时可能判断失误，事后应当有机会改变主意。承认撤回权，是对“信息自决”的贯彻。

比较法上，欧盟通用数据保护条例第七条第三款规定，撤回同意应当与作出同意一样

容易；撤回不影响撤回前处理的合法性。

我国第十五条的规定，与上述规则基本一致：有权撤回；处理者应当提供便捷的方式；撤回不影响撤回前基于同意的处理。

撤回的技术实现，可以有多种方式：设置中的“关闭”开关；隐私政策页面的“撤回”按钮；客服的“一键撤回”。

无论何种方式，都应当满足“便捷”的要求：步骤不超过同意时的步骤；不得要求提供额外的身份证明；不得设置不合理的等待期。

实务中，有的应用将“撤回”入口深埋于五级菜单，用户难以找到。此种设计，形式上提供了撤回方式，实质上剥夺了撤回权。

撤回的后果，是“停止处理”。但“停止”不等于“删除”：已收集的信息，可能因其他合法性基础而保留（如法定的保存义务）。

若信息主体要求删除，则须依第四十七条判断是否符合删除的条件；符合条件的，应当删除；不符合的，应当说明理由。

撤回后，处理者能否继续使用“已经去标识化”的信息？通说认为可以，因为去标识化后的信息，已不属于“可识别”的个人信息；但若可复原，则仍须停止处理。

须注意，撤回同意不影响“已经进行的处理”的合法性，也不影响“已经订立的合同”的效力。若处理系合同所必需，则撤回同意可能导致合同无法履行，处理者可以依合同法的规则处理。

六、撤回同意及其后果

个人信息保护法第十五条规定，基于个人同意处理个人信息的，个人有权撤回其同意；个人信息处理者应当提供便捷的撤回同意的方式。

撤回同意，是信息主体的法定权利，不得以约定排除。处理者不得以“同意不可撤回”条款，限制信息主体的权利。

撤回的方式，应当“便捷”。何为便捷？应当与同意的方式相当：若同意只需一次点击，则撤回也应当只需一次点击；不得要求书面申请、不得要求客服审核。

撤回的效力，是“向将来发生”。即：撤回前基于同意的处理，仍然有效；撤回后，处理者应当停止处理。

撤回后，处理者是否可以拒绝提供服务？依第十六条，不得拒绝，但处理属于服务所必需的除外。

“服务所必需”的判断，应当严格。若敏感个人信息的处理并非服务的核心功能，而只是附加功能（如个性化推荐），则不属于“所必需”。

例如，一款手电筒应用要求获取通讯录权限，该处理显然不属于“服务所必需”；用户拒绝后，应用不得拒绝提供照明功能。

须注意，撤回同意与“删除权”不同。撤回同意，只要求停止处理；删除权，要求删除已收集的信息。二者可以并用，但适用条件不同。

实务中，有的处理者以“技术上无法撤回”为由，拒绝提供撤回方式。此种抗辩，不能成立：技术上的困难，不能成为剥夺法定权利的理由。

例外情形的设置，是为了平衡“个人控制”与“社会利益”。若一律要求同意，则公共卫生、司法侦查、新闻报道等活动的开展，将受到严重阻碍。

但例外的适用，须严格把握：其一，须有法律明文规定；其二，须符合“必需”的要求；其三，须履行告知义务；其四，须采取保护措施。

以“履行法定职责”为例。公安机关为侦查犯罪而收集信息，属于法定职责；但收集的范围，应当限于与案件有关的范围。

以“新闻报道”为例。媒体为报道新闻而处理个人信息，属于公共利益；但报道应当“合理”，不得过度披露与报道无关的隐私。

以“已经公开的信息”为例。处理者处理个人自行公开的信息，可以不取得同意；但处理的，应当限于“合理范围”，不得超出公开的目的。

须注意，“已经公开”不等于“可以任意使用”。若公开的目的仅是“展示”，则将其用于“营销”，超出了合理范围。

司法程序中，法院调取个人信息，属于“履行法定职责”；但调取的范围，应当限于与案件有关的范围，且须履行相应的审批程序。

行政执法中，行政机关收集个人信息，须有法律、法规的依据；无依据的收集，即便以“执法”为名，仍属违法。

七、例外情形与豁免

敏感个人信息的处理，并非一律须取得单独同意。依第十三条的规定，下列情形无须取得同意：为订立、履行合同所必需；为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；依照本法规定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。

上述情形，同样适用于敏感个人信息。但适用时，应当严格把握“必需”的界限，不得以“合同必需”为由，扩大处理范围。

以“履行合同所必需”为例。若合同的核心义务是提供医疗服务，则收集患者的健康信息属于必需；但收集患者的行踪轨迹，则不属于必需。

以“应对突发公共卫生事件”为例。疫情期间收集健康码信息，属于必需；但收集个人的宗教信仰，则不属于必需。

须注意，例外情形只是免除“同意”，并不免除“告知”。处理者仍须依第十七条、

第三十条履行告知义务。

此外，第三十二条规定，法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。此即“特别法优先”。

例如，征信业管理条例对个人信用信息的采集、使用有特别规定；人类遗传资源管理条例对人类遗传资源的采集有特别规定。这些规定，优先于个人信息保护法的一般规则。

实务中，有的处理者以“已取得行政许可”为由，主张无须取得单独同意。此种主张，不能成立：行政许可与个人同意，是两个不同的合法性基础，不能相互替代。

个人信息保护法第六十九条规定，处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

该条确立了“过错推定”的规则：原告只须证明损害的存在，被告须证明自己没有过错。在单独同意的争议中，处理者须证明“已取得同意”，否则推定其有过错。

举证的内容，包括：同意的界面、同意的记录、告知的内容、撤回的方式、影响评估的报告。

实务中，有的处理者以“用户协议已勾选”作为证据，但未能提供勾选的具体记录。此种证据，不足以证明“该用户”已同意。

较为稳妥的做法是：采用“双记录”机制，既记录同意的文本，也记录同意的行为（时间、账号、网络地址、设备标识）。

检察公益诉讼中，举证责任的分配有所不同。检察机关代表公共利益，可以依职权调查取证；但处理者仍须就“已取得同意”承担证明责任。

合规的路径，还应当包括“内部制度”：设立个人信息保护负责人；制定处理规则；开展员工培训；建立投诉渠道；定期开展审计。

内部制度的价值，在于“预防”：与其在事后举证，不如在事前规范。制度的完善，是最好的抗辩。

八、举证责任与合规路径

举证责任的分配，是执法与诉讼的关键。依个人信息保护法的精神，处理者应当就其处理的合法性承担证明责任。

具体而言，处理者应当证明：已取得单独同意；同意的内容具体明确；已履行告知义务；已提供撤回方式；已采取严格保护措施。

未能证明的，推定为未取得同意。此种推定，符合“证据偏在”的原理：同意的记录由处理者掌握，信息主体难以证明“未同意”。

实务中，有的处理者以“后台有日志”为由主张已取得同意，但日志内容含糊，无法识别同意的具体范围。此种日志，不足以证明。

合规的路径，可以从四个方面着手：一是单独的告知界面，就每一项敏感信息的处理

单独说明；二是独立的勾选机制，用户须主动勾选，不得预设；三是可撤回的技术设计，在设置中提供“一键撤回”；四是影响评估的记录，依第五十五条进行事前评估并留存。

影响评估的内容，包括：处理的目的是否与必要性；对个人权益的影响；保护措施的有效性；风险与对策。评估报告应当留存三年以上。

须注意，影响评估不是“形式”，而是“实质”。若评估只是套用模板，未结合具体场景，则不能起到预防风险的作用。

合规的另一路径，是“最小必要”。即：只收集实现目的所必需的信息，不过度收集；只保存实现目的所必需的期限，不过度保存。

最小必要，是敏感个人信息处理的基本原则。其判断标准，是“实现目的所必需”，而非“有助于提升服务”。

类型七：智能汽车。车辆收集位置、驾驶行为、车内录音等信息，其中位置与车内录音属于敏感个人信息；处理须取得单独同意，并提供“关闭”选项。

类型八：可穿戴设备。手环、手表收集心率、睡眠、运动等健康信息，属于敏感个人信息；处理须取得单独同意，且不得将数据用于保险定价等无关目的。

类型九：校园管理。学校收集学生的面部信息用于考勤，属于敏感个人信息；须取得监护人的单独同意，并提供替代方案（如刷卡）。

类型十：网络招聘。平台收集求职者的健康、婚育等信息，属于敏感个人信息；除法律另有规定外，不得收集。

类型十一：人脸支付。支付机构采集人脸信息，须取得单独同意；且须提供“密码支付”等替代方式，不得强制“刷脸”。

类型十二：社区治理。物业采集业主的人脸、车牌信息，须取得单独同意；业主有权拒绝，并选择其他验证方式。

类型化的意义，在于把抽象的规则落到具体的场景。场景清晰，合规便有抓手；场景模糊，合规便流于形式。

九、实务中的类型化

类型一：人脸识别。人脸信息属于生物识别信息，处理须取得单独同意；公共场所安装图像采集设备，须遵守第二十六条的规定，只能用于维护公共安全，不得用于其他目的。

实务中，有的小区以“门禁”为由，强制业主录入人脸。此种做法，不符合单独同意的要求；业主有权选择其他验证方式（如门禁卡）。

类型二：医疗健康信息。医院收集患者的病历、检验报告，属于“履行合同所必需”，可以不取得单独同意；但将病历用于科研，则须取得单独同意。

类型三：金融账户信息。银行收集客户的账户信息，属于“履行合同所必需”；但将

账户信息用于营销，则须取得单独同意。

类型四：行踪轨迹。地图应用收集用户的位置，属于“服务所必需”；但持续在后台收集位置，则超出了必要的范围。

类型五：未成年人信息。教育类应用收集学生的信息，须取得监护人的单独同意，并制定专门的保护规则。

类型六：工作场所监控。用人单位在办公场所安装监控，涉及员工的个人信息；其合法性，须依“劳动合同所必需”与“告知同意”双重标准判断。

类型化的意义，在于明确不同场景下的合规要求。场景不同，必要性不同，同意的要求也不同。笼统适用同一标准，难免削足适履。

回望全文，可以发现一条主线：单独同意的规则，本质上是“程序正义”在数据领域的体现。程序不能保证结果一定正确，但可以保证结果可以被接受。

我国个人信息保护法实施数年，执法力度逐步加强，企业的合规意识显著提高。但“形式合规、实质违规”的现象，仍然存在。

解决的办法，不在于增加更多的形式要求，而在于强化“实质审查”：同意是否真实、告知是否充分、撤回是否便捷、处理是否必要。

对法官而言，重要的或许不是记住多少条文，而是理解条文背后的价值：个人信息不是“石油”，而是“人格的延伸”；处理个人信息，不是“开采资源”，而是“介入他人的生活”。

把握住这一点，裁判便有了方向：在技术创新与人格保护之间，寻找平衡；在效率与尊严之间，守住底线。

还有一层考虑，值得指出。同意的规则，看似是“程序技术”，实则关乎“权力结构”：处理者掌握技术与信息，个人处于弱势；同意规则的功能，正是通过程序，矫正这种不对等。

矫正的方式，不是否定技术，而是让技术“可见”：让个人知道信息被谁收集、用于何处、保存多久。可见，才能选择；选择，才能自主。

由此观之，单独同意的“单独”二字，不只是形式的要求，更是一种态度：把对方当作有判断能力的主体，而不是可以随意处置的数据来源。

态度的转变，比规则的增加更为根本。规则可以被规避，态度却会渗透到产品的设计、流程的安排、界面的措辞之中。

愿每一次设计的背后，都有对人的尊重；愿每一次点击的背后，都是真实的选择。此即本文的期许。

技术上，单独同意并非难事：一个独立的弹窗、一次主动的勾选、一条清晰的说明，成本甚低。难的是愿不愿意做，而不是能不能做。

当企业把“用户体验”理解为“减少打扰”时，单独的弹窗便被视为负担；当企业把

“用户体验”理解为“尊重选择”时，弹窗便成为服务的一部分。理解的差异，决定了设计的差异。

监管的意义，正在于通过规则，推动理解方式的转变：让尊重成为常态，让敷衍付出代价。规则的力度，最终体现为态度的转变。

最后，须重申一点：同意不是“卖身契”，也不是“免责单”。它只是处理者与个人之间的一次对话，对话的前提是平等，对话的结果是授权。失去了平等，同意便只剩形式。

平等不是抽象的口号，它体现在每一行说明的文字里、每一个默认的设置里、每一次撤回的点击里。细节之处，最见真章。

制度的进步，往往不是靠一次宏大的改革，而是靠无数次细微的修正。每一次修正，都是对尊重的重申。

十、结语

敏感个人信息的单独同意，可以概括为三句话：单独是形式，有效是实质，撤回是保障。形式使同意可识别，实质使同意真实，保障使同意可反悔。

本文的三个主张，都围绕“真实”展开。三重含义解决“如何单独”的问题，四项要件解决“是否有效”的问题，撤回机制解决“能否反悔”的问题。三者依次展开，同意便从“形式合规”变为“实质自主”。

对处理者而言，这一框架的实益是合规的路径：单独告知、独立勾选、便捷撤回、影响评估。路径清晰，合规的成本便可预期。

对信息主体而言，这一框架的实益是选择的真实：其可以知情，可以选择，可以反悔。选择的真实，是人格自主的体现。

对社会而言，这一框架的实益是信任的建立。数字经济的发展，依赖数据的流通；但流通的前提，是信任。没有信任的流通，终将枯竭。

最后须指出，同意的本质，是“尊重”。尊重信息主体的知情，尊重其选择，尊重其反悔。技术的进步，不应以牺牲尊重为代价；制度的完善，应当以增进尊重为目标。

愿每一次点击都出于知情，每一次授权都出于自愿，每一次撤回都得到尊重。此即个人信息保护的本意。

参考文献

- [1] 《中华人民共和国个人信息保护法》第十三条、第十四条、第十五条、第十六条、第十七条、第二十三条、第二十五条、第二十六条、第二十八条、第二十九条、第三十条、第三十一条、第三十二条、第五十五条。
- [2] 《中华人民共和国民法典》第一千零三十四条、第一千零三十五条、第一千零三十六条。
- [3] 《信息安全技术 个人信息安全规范》（国家标准第35273号，2020年）。
- [4] 《移动互联网应用程序个人信息保护管理暂行规定》。

- [5] 程啸：《个人信息保护法理解与适用》，中国法制出版社2021年版。
- [6] 张新宝：《个人信息处理中的同意规则》，《中国法学》2021年第4期。
- [7] 王锡铎：《敏感个人信息的法律保护》，《法学研究》2022年第3期。