

个人信息保护法 企业合规启示报告

上篇

个人信息处理新变局

SFC 南方财经全媒体集团
Southern Finance Omnimedia Corp.

21世纪经济报道 | 21财经
21st CENTURY BUSINESS HERALD | 掌握全球财经脉搏

南方财经全媒体集团合规科技研究院

前言

近年来,伴随着数字经济发展,对个人信息的采集和利用成为一种“刚需”。个人信息保护不断涌现出新问题,随意收集、违法获取、过度使用、非法买卖个人信息等情况“野火烧不尽”。信息数据的挖掘利用与个人保护之间张力扩大,急需专门法律对个人信息处理活动提供规范样本。

放眼全球,个人信息保护立法在如火如荼地展开,目前已经有 128 个国家通过立法保护个人信息和隐私。欧盟《通用数据保护条例》、美国加利福尼亚州隐私保护法的出台,在国际上颇具影响力。

《个人信息保护法》在此背景下被纳入立法进程,并在各方推动下不断提速,千呼万唤始出来。2021年8月20日,《中华人民共和国个人信息保护法》由第十三届全国人民代表大会常务委员会第三十次会议通过,自2021年11月1日起施行。

《个人信息保护法》共 8 章 74 条。在有关法律的基础上,该法进一步细化、完善个人信息保护应遵循的原则和个人信息处理规则,明确个人信息处理活动中的权利义务边界,健全个人信息保护工作体制机制。该法成为我国迈入数字化社会,彰显“以人为本”的法律制度里程碑,也是我国为全球数字治理贡献的中国方案。

南方财经全媒体集团合规科技研究院长期关注个人

信息保护议题,持续跟踪报道立法进程、监管动态、公众呼声。借《个人信息保护法》落地之际推出解读报告,分析当前“大数据杀熟”、强制同意、人脸识别、超大型平台义务等多项热点。

报告分为上下两篇,上篇《个人信息处理新变局》梳理立法路径与模式,聚焦个人信息处理逻辑的转变,下篇《企业风险研判》则将目光放到企业合规的重点与难点,以及新的信息处理机制在数字经济发展中面临的新挑战。

本篇将展现近 20 年来个人信息保护的不断完善与发展;厘清个人信息相关概念;拆解“告知—同意”为核心原则的个人信息处理规范,解读围绕这一核心规则给企业带来的信息处理模式变革。

版权声明

本报告版权为南方财经全媒体集团合规科技研究院所有,并受法律保护。其他媒体、网站或个人以转载、摘编或其他方式使用本报告内容的,必须注明“来源:南方财经全媒体集团合规科技研究院”字样,否则不得进行商业性的原版原式转载,也不得歪曲和篡改本报告所发布的内容。违反上述声明者,我们将依法追究其相关法律责任。

目录

- P01 / 一、背景**
 - P01 / (一)个人信息保护的立法时间表(2009-2021)
 - P04 / (二)关于个人信息处理的其他立法
 - P05 / (三)相关概念厘清
 - P05 / 1. 个人信息、隐私与敏感个人信息
 - P06 / 2. 去标识化、匿名化

- P07 / 二、企业处理个人信息模式的变革**
 - P07 / (一)“告知-同意”处理规则
 - P08 / 1. 现实困境
 - P09 / 2. 信息处理模式转变
 - P09 / 3. 合规要点
 - P13 / (二)自动化决策
 - P13 / 1. 确立算法自动化决策治理框架
 - P14 / 2. 信息处理者责任增加
 - P16 / 3. 合规要点
 - P17 / 4. 落地难点
 - P18 / (三)撤回同意
 - P19 / 1. 对信息处理者要求更严格
 - P19 / 2. 合规要点
 - P20 / (四)删除权
 - P20 / 1. 课以信息处理者更重义务
 - P22 / 2. 合规要点
 - P23 / (五)“告知-同意”之外情形
 - P23 / 1. 同意的例外情形
 - P25 / 2. 告知的例外情形

- P33 / 学术指导**
- P33 / 致谢**

一、背景

纵观《个人信息保护法》立法路程，走过近二十年。这期间，互联网高速发展，大数据时代来到。伴随着高频、高速、高密度的数据交流传输，作为原材料的个人信息的滥用问题相伴而至。这些年，对个人信息保护的立法呼声越来越高，急需一部专门法律定分止争。《个人信息保护法》应运而生。

(一)个人信息保护的立法时间表(2009-2021)

我国《个人信息保护法》的立法时间跨度长。2003年，彼时的国务院信息化办公室部署立法研究工作，2005年，相关学者完成《个人信息保护法(专家建议稿)》，但受多重因素的影响，《个人信息保护法》一度陷入停滞。

2009年至2018年，关于个人信息保护的规定零星散落于多部法律中。2017年，受全国人大法工委和中央网信办委托，中国社会科学院法学研究所副所长、研究员周汉华起草了《个人信息保护法(专家建议稿)》。

2018年，《个人信息保护法》被纳入十三届全国人大常委会立法规划，正式拉开立法序幕；2020年10月，第十三届全国人大常委会第二十二次会议对《个人信息保护法(草案)》进行首次审议，至2021年8月17日，《个人信息保护法(草案)》进入三审。同年8月20日，十三届全国人大常委会第三十次会议表决通过《个人信息保护法》，自2021年11月1日起施行。

《个人信息保护法》立法时间表（2009-2021）

2009年2月28日

《刑法修正案（七）》新增第253条之一，将窃取或以其他方式非法获取公民个人信息、出售或非法提供公民个人信息的情节严重的行为规定为犯罪。

2012年12月28日

《全国人民代表大会常务委员会关于加强网络信息保护的决定》，明确“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”。

2013年6月28日

《电信和互联网用户个人信息保护规定》界定“用户个人信息”概念，规定信息收集和使用规范、安全保障措施、监督检查等内容。

2014年3月15日

新修改的《消费者权益保护法》实施，将个人信息得到保护的权力列为消费者的一项基本权利。

2015年11月1日

刑法修正案（九）施行，扩大个人信息相关罪名适用范围，不再限定于特定履职人员，提高量刑。

2016年11月7日

《网络安全法》设立“网络信息安全”章节，个人信息作为重要的组成部分。

2017年10月1日

《民法总则》施行，明确自然人的个人信息受法律保护。

2018年8月27日

《民法典》各分编草案提请审议，人格权独立成编，明确个人信息的定义；收集个人信息应当遵循的原则；保证个人信息的存储安全等。

(续上表)

《个人信息保护法》立法时间表 (2009-2021)

2018年9月7日

十三届全国人大常委会立法规划公布,《个人信息保护法》在列,有望在五年内提请审议。

2019年5月28日

《数据安全管理办法》公开征求意见,对数据收集、处理使用和安全监督管理都提出了要求。

2019年6月13日

《个人信息出境安全评估办法》公开征求意见,规定个人信息出境应进行安全评估,对个人信息出境进行限制。

2019年8月22日

《民法典》人格权编草案(三审稿)提交全国人大常委会审议。

2019年10月1日

《儿童个人信息网络保护规定》施行。这是我国第一部专门针对儿童的网络保护规范,抵制可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等违法信息。

2019年12月20日

全国人大常委会法工委发言人岳仲明介绍2020年立法工作安排,《个人信息保护法》将于明年制定。

2020年5月14日

新华社消息称,《个人信息保护法》正在研究起草中,草案稿已经形成,将尽早提请全国人大常委会会议审议。

2020年5月25日

全国人大常委会工作报告在下一步主要工作安排中指出,将制定个人信息保护法、数据安全法等。

(续上表)

《个人信息保护法》立法时间表 (2009-2021)

🕒 2020年5月28日

十三届全国人大三次会议表决通过了《民法典》，自2021年1月1日起施行。

🕒 2020年10月13日

《个人信息保护法草案》进行了首次审议，内容包括健全个人信息处理规则、个人的权利和处理者义务、履行个人信息保护职责的部门等。

🕒 2021年4月26日至29日

《个人信息保护法草案（二次审议稿）》提交审议，针对个人信息收集、使用规则不透明及过度收集、使用等问题进一步完善。

🕒 2021年6月10日

十三届全国人民代表大会常务委员会第二十九次会议通过《数据安全法》，自2021年9月1日起施行。

🕒 2021年8月17日

《个人信息保护法草案》提请三审，对APP过度收集个人信息、“大数据杀熟”等作出规范，将不满十四周岁未成年人的个人信息作为敏感个人信息。

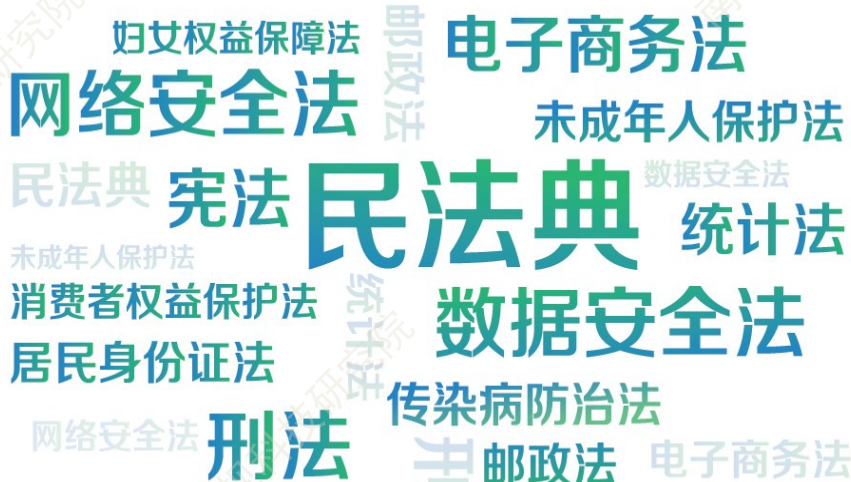
🕒 2021年8月20日

十三届全国人大常委会第三十次会议表决通过《个人信息保护法》，自2021年11月1日起施行。

(二)关于个人信息处理的其他立法

过去,我国已有多部法律文件涉及个人信息处理,这些规范比较分散,呈现出碎片化的特征。

如《宪法》《民法典》分别规定了“公民的通信自由和通信秘密”“自然人的个人信息”受法律保护,《刑法》确定了侵犯个人信息的相关罪名,《数据安全法》《网络安全法》等也有对个人信息保护大篇幅的规定,详细法律法规条款参见报告附录。



(三)相关概念厘清

1. 个人信息、隐私与敏感个人信息

《民法典》将隐私定义为:自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。在第 1034 条第 3 款个人信息的定义下,区分了私密信息和非私密信息,“个人信息中的私密信息,适用有关隐私权的规定;没有规定的,适用有关个人信息保护的规定。”

个人隐私与个人信息呈交叉关系,即有的个人隐私属于个人信息,而有的个人隐私则不属于个人信息;有的个人信息特别是涉及个

人私生活的敏感信息属于个人隐私,但也有一些个人信息因高度公开而不属于隐私^①。

《个人信息保护法》第二十八条将敏感个人信息定义为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。

敏感信息与个人信息的区别在于,前者是“一旦泄露或非法使用”,就容易造成个人名誉、身心健康受到损害或歧视性待遇等,因此立法对其的保护标准更为严格。

2. 去标识化、匿名化

匿名化的三个要件:一是个人信息必须经过处理,二是处理后的数据无法识别特定自然人,三是数据不能复原^②。

这一概念在《个人信息保护法》中得到明确:“匿名化是指个人信息经过处理无法识别特定自然人且不能复原的过程”。

根据《信息安全技术 个人信息去标识化指南》(GB/T 37964-2019),去标识化的定义为通过对个人信息的技术处理,使其在不借助额外信息的情况下,无法识别个人信息主体的过程。《个人信息保护法》保留了该定义,表述为“个人信息经过处理,使其在不借助额外信息的情况下无法识别特定自然人的过程。”

去标识化和匿名化都是个人隐私安全的技术防护手段,二者的主要区别在于,去标识化后的信息也属于个人信息,如果与其他额外信息结合,可以识别个人信息主体,通常也称为重标识;而匿名化处理之后,个人信息控制者不能直接或间接地再次识别个人信息,匿名化后的信息不属于个人信息,且无法与额外信息结合识别出个人信息主体。

二、企业处理个人信息模式的变革

理解个人信息保护，必须先理解个人信息权在中国语境下的含义。个人信息权具有控制自己信息的积极权利面向。个人具有知情、同意、删除等权利，有权控制信息处理者、运营者如何使用自己的信息^③。

《个人信息保护法》立法贯穿“信息自决”主线，体现在赋予个人同意撤回、决定权、查阅权、复制权、更正权、删除权等方面^④。最终新增的“数据可携带权”也给予了个人自主权，个人在面对信息处理者的不平等地位差距时，拥有了与其抗衡的“武器”。这也给企业的个人信息处理逻辑带来变化。



(一)“告知-同意”处理规则

“告知-同意”原则，指信息处理者在收集个人信息时，应当对信息主体就有关个人信息被收集、处理和利用的情况进行充分告知，并征得信息主体明确同意的原则^⑤。

早在2012年，《全国人民代表大会常务委员会关于加强网络信息保护的決定》首次在法律文件中确定了个人信息收集的“用户同意原

则”^⑥。近年来，随着《网络安全法》和《民法典》等法律法规的出台，“告知-同意”原则已发展成为我国目前个人信息保护最主要的合法性基础。

《个人信息保护法》也将“告知-同意”确立为个人信息处理规则的核心。但是，“告知-同意”这项基础原则在实操场景中会遇到各类现实问题，有时甚至无法实现。

1. 现实困境

1.1“隐私政策”无人读、不可读、读不懂^⑦

国外有研究成果表明，如果用户要阅读提供给他们的所有隐私政策，每年需平均付出 244 个小时；如果只是粗略阅读，每年需平均付出 154 个小时。

这意味着，每人将平均每天花费 40 分钟阅读和理解各企业的隐私政策。如果计入准确理解所需的时间、专业知识和精力，那么这一“知情”的成本更为高昂^⑧。

不少隐私政策专业性、复杂性高，信息处理者内部可以循环解释。如果用户无法全面知悉其同意内容，实践中可能陷入损害救济困境，司法实践中已有相关案例。

1.2 被“胁迫同意”难以行使拒绝权^⑨

当前，很多企业的隐私政策在页面呈现及设计上不规范，存在只有“同意”按钮或不同意无法使用产品或服务的情况。

即使用户仔细阅读了隐私政策，但在作出个人信息利用的许可决定时，往往缺乏选择的空间，只有一种全有或全无的选择状态。

1.3 多方流转中知情权无法保障

在个人信息密集收集与多方流转的生态系统中,用户在很多情况下对其信息的收集并不知情,难以对第一方收集者行使权利,更遑论向缺乏直接联系的第三方机构行使控制权^⑩。

2. 信息处理模式转变

“告知-同意”原则是个人信息保护机制中的基础原则,信息处理者基于该规则进行信息收集、存储、使用、加工、传输、提供、公开等,赋予了信息主体对个人信息较为绝对的支配权利,一定程度上将改变企业对个人的非对称强势权力。

从监管层面来看,相关执法监管近年来更为严格。工信部、网信办等相关部门对信息处理活动的规范与约束更为细化。

面对立法闸口的收紧以及现实的监管趋势,作为信息处理者的企业在处理个人信息的逻辑需重塑。

3. 合规要点

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。

“告知-同意”规则下的“告知”形式

需告知

个人信息处理者的名称或者姓名和联系方式

个人信息的处理目的、处理方式，处理的个人信息种类、保存期限

个人行使本法规定权利的方式和程序

法律、行政法规规定应当告知的其他事项

规定事项发生变更的，应当将变更部分告知个人

涉及敏感信息，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

告知以外情形

有法律、行政法规规定应当保密或者不需要告知的情形的

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知

3.1 告知方式改进

表现形式需“显著”、清晰易懂，真实、准确、完整地向个人告知。

企业应以个人容易辨识且易于获取的方式进行告知，告知内容应当显著地出现在用户可能看见的界面之中，且这种看见的可能性应当是合理的^①。

3.2 告知内容完善

需告知个人信息收集行为的主体，不仅包括信息控制者，还应包括其余参与、辅助或者能直接经采集而获取用户行为信息的主体；行为信息的类别和使

用目的;采集后的处理行为;用户行为信息流向的第三方^②。

建议个人信息收集的“告知”在内容渐进,具备一定的层次。第一层次的告知应在收集行为本身。企业应向用户说明收集主体、被收集信息的属性和内容,以及所使用自动化采集工具的基本功能等情况。第二层次的告知应深入收集后自动化处理的层面,将对行为信息后续利用环节带来的不确定性和潜在风险毫无保留地充分告知用户。

3.3 不同场景下细化

不同信息需要不同的收集模式,放置于不同场景下,建构场景与风险导向的个人信息保护新路径。例如,《个人信息保护法》对于单独同意的敏感信息,单设一章予以专门规范。

企业应从个人信息的敏感度、场景进行风险分析,基于处理行为的类型去区别实施不同的同意方式^③,并为实现不同的同意匹配新型的同意机制。

“告知-同意”规则下的“同意”形式

同意

普通个人信息



单独同意

- 向其他个人信息处理者提供其处理的个人信息的
- 在公共场所安装图像采集、个人身份识别设备收集的
个人图像、身份识别信息用于除“维护公共安全”以外的其他目的
- 敏感个人信息
- 向境外提供个人信息
- 法律、行政法规相关规定



书面同意

- 法律、行政法规相关规定



重新同意

- 个人信息处理目的、处理方式和处理的个人信息种类发生变更
- 个人信息处理者需要转移个人信息，接收方变更原先的处理目的、处理方式
- 个人信息处理者向其他个人信息处理者提供其处理的个人信息，接收方变更原先的处理目的、处理方式。



父母或其他 监护人同意

- 处理不满十四周岁未成年人个人信息的



撤回同意

- 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
- 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
- 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
- 个人信息处理者应当主动删除个人信息

(二) 自动化决策

算法是数字平台处理海量用户数据、绘制用户画像、精准定价与个性化推送的“生产工具”，已经成为平台运行的核心动力。

随着十余年平台经济的高速发展，算法自动化决策的滥用与伦理缺失的累积危害已经进入了显现期^④。

《个人信息保护法》从一审稿到成文，在不断强化对自动化决策的规制，回应社会关切。最终明确：“自动化决策应保证透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。”

1. 确立算法自动化决策治理框架

随着算法的广泛应用引发的虚假信息、用户隐私、信息茧房、算法歧视等负面影响的持续发酵，我国相关立法和标准开始关注算法推荐^⑤。

评价分选、价格歧视、“大数据杀熟”等由用户画像或其他自动化决策带来的影响，被视为有损害人格尊严、人格自由的危险；并且，伴随着算法对日常生活的渗透，其一定程度上涉及社会治理问题，深远地影响公共利益。

毫无疑问的是，技术中立与无差别技术抗辩已经无法成为平台规避责任的面纱，算法背后体现的是设计者意志，算法自动化决策的风险是平台内生的。

《个人信息保护法》回应社会对算法的关注，确立我国算法自动化决策治理的基本框架。平台作为最重要的自动化决策的主体，须承担事前风险预防义务、事中安全运行义务与事后的相关责任。

2. 信息处理者责任增加

“自动化决策”相关要求

不得对个人在交易价格等交易条件上实行不合理的差别待遇

决策的透明度和结果公平、公正

评估、记录处理情况

向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式

作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定

2.1 事前评估

《个人信息保护法》将平台算法治理时点前移。第五十五条确立了自动化决策的事前评估制度，要求个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录。

算法自动化决策的风险是平台内生的，伴随着平台作为设计者的决策与行为，依赖事后追责机制，可能会造成未来不断出现平台新的算法自动化决策治理缺位。

2.2 相关义务增加

“自动化决策”各次审议及全文对比

| 一审稿 | 二审稿 | 通过版 |
|---|---|---|
| 应当保证决策的透明度和处理结果的公平合理。 | 应当保证决策的透明度和结果公平合理。 | 应当保证决策的透明度和结果 公平、公正 。 |
| | | 不得对个人在交易价格等交易条件上实行不合理的差别待遇。 |
| 通过自动化决策方式进行商业营销、信息推送,应当同时提供不针对其个人特征的选项。 | 通过自动化决策方式进行商业营销、信息推送,应当同时提供不针对其个人特征的选项,或者向个人提供 拒绝的方式 。 | 通过自动化决策方式向个人进行信息推送、商业营销,应当同时提供不针对其个人特征的选项,或者向个人提供 便捷的拒绝方式 。 |
| 个人认为自动化决策对其权益造成重大影响的,有权要求个人信息处理者予以说明,并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。 | 通过自动化决策方式作出对个人权益有重大影响的决定,个人有权要求个人信息处理者予以说明,并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。 | 通过自动化决策方式作出对个人权益有重大影响的决定,个人有权要求个人信息处理者予以说明,并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。 |

2.2.1“大数据杀熟”被禁止

《个人信息保护法》第二十四条要求“不得对个人在交易价格等交易条件上实行不合理的差别待遇”,或指向近年来备受关注的“大数据杀熟”。利用算法进行“不合理的差别待遇”被法律禁止,信息处理者义务增强。

此前,我国已从反垄断的制度框架下对歧视性定价问题进行了规

范。《反垄断法》第十七条规定,禁止具有市场支配地位的经营者没有正当理由,对条件相同的交易相对人在交易价格等交易条件上实行差别待遇。

《个人信息保护法》增加了“大数据杀熟”条款,进一步丰富了对歧视性定价问题的规制路径。按照《个人信息保护法》的规定,无论个人信息处理者是否具有市场支配地位,只要个人信息处理者利用个人信息进行自动化决策,对个人在交易价格等交易条件上实行不合理的差别待遇,就是法律所禁止的行为^⑥。

2.2.2 信息处理者责任负担增加

《个人信息保护法》一审稿中要求“个人认为自动化决策对其权益造成重大影响的,有权要求个人信息处理者予以说明”。“个人认为”依赖于个人对算法的警惕与自主意识,不同人的认知差可能会导致该条款的约束性不足。此后二审稿删除“个人认为”这一表述,把责任主体转移到了信息处理者身上。

《个人信息保护法》还明确,在决策对个人权益造成重大影响时赋予个人主体拒绝权,“向个人提供便捷的拒绝方式”。不仅赋予个人主体拒绝权,并且需提供“便捷”的拒绝方式,对信息处理者有较强的制约。

《个人信息保护法》将平台算法治理时点前移,治理手段升级,相关义务增加,初步确立了算法问责制的基本框架^⑦。算法透明和算法公平,不仅是道德层面的要求,亦是法律义务。

3. 合规要点

3.1 算法透明

目前,基于算法自动化推荐而提供个性化信息内容服务已然逐渐成为各类 APP“标配”,为了更多样化地满足各类用户的使用需求,追

求定制化、独特性的移动互联网应用，必须依赖于“用户画像”等类似技术实现数据驱动与用户增长，培养流量黏性[®]。

企业需进一步完善自己的隐私政策，告知个人信息的收集会被用于用户画像和个性化展示，并征得用户的同意，充分保障用户知情权。在正式进行自动化决策前，应当就自动化决策的透明和公平性做好充分说明。

随着用户自主控制权提升，《个人信息保护法》要求信息处理者需提供“便捷”的拒绝方式，这也意味着企业需优化相关设置，包括提供直观的关闭和退出选项、在用户选择退出后对相关个人信息进行删除、提供相应的投诉机制。

3.2 最小化处理原则

用户画像的处理已经越来越精细，推荐与服务也越来越精准。这不可避免会造成用户个人信息收集、使用程度超出必要性、商家的供应商或关联方违法向其他第三方提供用户个人信息进行获利的问题[®]。

企业进行自动化决策，需遵循重申目的明确和最小化处理原则。随着 2021 年 3 月正式出台的《常见类型移动互联网应用程序必要个人信息范围规定》，个性化推荐所依赖的“设备信息、广告标识符”等并未作为必要个人信息类型予以规定，“最小化处理原则”是自动化决策的重要原则，企业应遵循该原则进行信息处理。

4. 落地难点

虽然《个人信息保护法》强化对算法规制，但能否落地待考证。

“利用个人信息进行自动化决策，应当保证决策的透明度和处理

结果的公平合理”，但未进一步解释应如何履行。事实上“透明”和“公平合理”是很主观的，不同的人会有不同的理解，而差异化的理解可能导致实践中对该义务的履行程度不一。

针对上述问题，或可对互联网平台企业建立外部监督渠道，监督其算法规则制定。

（三）撤回同意

同意撤回，指个人信息主体基于“告知-同意”原则，对自己已经作出的“同意信息处理者对其个人信息进行处理”的授权予以取消的意思表示。实质含义为意思表示的撤销。同意的撤回包含个人信息主体对个人信息使用全过程中的处分⁹⁰。

同意撤回权体现了主体对于个人信息的自决处分，可以被定性为 人格权体系下的撤销权。撤销权可被视为在信息处理活动中，个人防御性的信息权益，对信息处理进行暂停式的缓冲效力，可对冲部分个人信息处理对人格权益的侵害效果。

“撤回同意”相关要求

“撤回同意”相关要求

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

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

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

个人信息处理者应主动删除个人信息

1. 对信息处理者要求更严格

同意撤回权已经成为全球个人信息保护立法的趋势与共识,《个人信息保护法》中也对此进行了回应。

根据《个人信息保护法》规定可知,用户行使撤回同意权利的时间不限于信息的收集阶段,因为在同意收集个人信息的初始阶段,个人往往很难理解、判断做出该同意将面临何种后果。撤回同意可以在个人信息的收集、使用、保存、共享等全生命周期内行使。

此次将“撤回同意”升格至法律,显示了立法者更严格的保护态度。

2. 合规要点

目前主流撤回同意有两种模式,一是在产品中设计按钮,点击撤回同意的选项即可实现,二是通过电话、邮箱等人工方式撤回同意。实践中存在撤回同意不够方便,使用户最终不了了之的情形^②。

《个人信息保护法》二审稿中对撤回同意增加“便捷”的要求,与欧盟《通用数据保护条例》GDPR“撤回同意应当和表示同意一样简单”的宗旨以及《个人信息安全规范》等相关规定相呼应。

为响应并处理个人同意的撤回请求,企业需调整现有的业务流程,通过技术工具的支持将合规流程自动化;向消费者明示撤回同意的方法,确保该方法简单易操作、且能及时获得企业的响应。

个人撤回同意之后,数据处理的合法基础不复存在,个人信息处理者需要立即停止数据处理行为,应按照《个人信息保护法》的具体规定进行处理,否则将面临不利的法律后果。

(四) 删除权

信息删除权是指个人一定条件下能够针对信息处理者提出删除某些个人数据的权利。《个人信息保护法》中赋予了个人这一权利，加强保护个人隐私、防范风险，并且作为调整个人与信息处理者力量差异的砝码，消弭双方之间不平等。

1. 课以信息处理者更重义务

“删除权” 相关法律



侵权责任法



(2010年7月1日起施行； 2021年1月1日起废止)

● 第三十六条

网络用户、网络服务提供者利用网络侵害他人民事权益的，应当承担侵权责任



网络安全法



(2017年6月1日起施行)

● 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



民法典



(2021年1月1日施行)

● 第一千零三十七条

自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除

(续上表)

“删除权” 相关法律



个人信息保护法

(将于**2021年11月1日**施行)

- **第四十七条：** 有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除

处理目的已实现、无法实现或者为实现处理目的不再必要

个人信息处理者停止提供产品或者服务，或者保存期限已届满

个人撤回同意

个人信息处理者违反法律、行政法规或者违反约定处理个人信息

法律、行政法规规定的其他情形

- **第四十七条（替代履行方式）**

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理

- **第四十九条**

自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利

2010年施行的《侵权责任法》赋予了个体请求删除个人信息的权利,但这种权利的行使仍然以存在“侵权行为”为前提^②。

此后,《网络安全法》《民法典》等立法中不断加强对个人信息保障,做出个人信息删除的相关规定,但还是基于“个人发现信息处理者违反相关法律法规、双方规定”。

《个人信息保护法》则明确赋予了个人删除权利,扩大了个人行使删除权的情形。并且,对信息处理者课以更严格的义务,信息处理者应当主动或者根据个人的请求删除,将相应个人信息的删除定位为经营者应当主动履行的义务。

此外,《个人信息保护法》对个人信息处理者提出了一项类似“行为中止”的删除权救济保障,即,如果个人信息主体要求行使删除权但实际上保存期限尚未届满,或技术上存在很大困难的,则个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

2. 合规要点

2.1 建立删除实现机制

目前,信息处理者对响应个人删除权仍存在不足。以APP运营商为例,隐私政策关于用户删除权的规定分散且简短;此外,许多运营商之间存在信息流通和共享,用户为获取相关服务不得不概括接受运营商包含“将从第三方或其他来源收集用户个人信息”的隐私政策,但其删除个人信息的诉求若只到达运营商而无法企及第三方,删除权行使的有效性就会大打折扣^③。

《个人信息保护法》落地后,企业需建立完善的删除实现机制。

在用户自行操作删除个人信息的情形下,企业应当阐明个人信息

删除权的实现机制,展示具体示例来辅助用户操作。

在隐私政策以及呈现方式上进一步完善,企业应对涉个人信息删除权的内容根据重要性对字体、格式、注释等作出调整,后台设置显著、明晰的流程指导、服务用户行使删除权。

2.2 完善风险评估机制

个人信息的删除涉及场景多,除了个人自身以外,可能涉及其他利益主体。企业需仔细研判其中的法律风险,设计合理的评估机制,在信息处理各流程中识别风险,积极响应。

个人申请删除个人信息后,企业数据处理的合法性基础不复存在。如删除难以实现,运营商是否继续存储全部或部分个人信息、是否匿名化处理继续存储的信息及其安全保障程度、彻底删除个人信息的期限和程序等,均需做出后续处置说明。

(五)“告知-同意”之外情形

考虑到实践中个人信息处理情况的多样性,《个人信息保护法》对无需告知以及个人同意以外合法处理个人信息的情形作了规定。

1. 同意的例外情形

《个人信息保护法》拓展了《民法典》第一千零三十六条告知同意的两项免责事由,确定了6种同意的例外情形:

同意的例外情形

同意的例外情形

- 为订立、履行个人作为一方当事人的合同所必需
- 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
- 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
- 法律、行政法规规定的其他情形

1.1 个人信息处理空间更灵活

由于存在的利益众多，如公共利益、法定职责、国家利益、自然人的生命健康和财产安全，所以，法律和行政法规上规定的不需要同意的情形同样较多。“同意+例外”规制方式，给予了个人信息处理更灵活的空间。

1.2 员工信息保护存争议

在无需同意的情形中，最终《个人信息保护法》新增：依照依法制定的劳动规章制度和依法签订集体合同实施人力资源管理所必需。

员工个人信息的保护在实践中一直争议较大，在企业的日常人力资源管理中，从招聘到员工离职，全环节均涉及员工个人信息的收集、

存储、使用和传输。正式稿这一新增条款对于企业而言提供了明确的适用准则,将人力资源管理所必需的场景限缩于“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”这两大场景之下²⁹。

但是给企业开的这扇“无需同意”的后门在实践中是否会被滥用,仍待观察。

2. 告知的例外情形

与同意规则一样,告知规则也有不适用的情形,即在特定的情形下,处理者不负有告知的义务。

在个人信息处理中,免除告知义务的情形和无须同意的情形存在差别。告知义务的履行既有利于维护个人的知情权,也完全不会如同同意规则那样构成对处理者实施个人信息处理活动的法律障碍。故此,法律上对于免于告知的情形应当作更加严格的限制³⁰。

附录

关于个人信息处理的其他立法

《宪法》

第二章 “公民的基本权利和义务”

第四十条 中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。

《民法典》

总则编第五章 “民事权利”

第一百一十一条 自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

第四编 “人格权编” 第六章 “隐私权与个人信息保护”

对个人信息的概念和类型、个人信息保护与隐私权的关系、处理个人信息应当遵循的原则与告知同意规则、自然人对其个人信息享有的权益内容、处理个人信息的免责事由，信息处理者的法定义务等作出了系统的规定。

《刑法》

第二编 “分则” 第四章 “侵犯公民人身权利、民主权利罪”

第二百五十二条 【侵犯通信自由罪】
第二百五十三条 【私自开拆、隐匿、毁弃邮件、电报罪】
第二百五十三条 之一 【侵犯公民个人信息罪】

第六章 “妨害社会管理秩序罪” 第一节 “扰乱公共秩序罪”

第二百八十五条 【非法侵入计算机信息系统罪】【非法获取计算机信息系统数据、非法控制计算机信息系统罪】【提供侵入、非法控制计算机信息系统程序、工具罪】
第二百八十六条 之一 【拒不履行信息网络安全管理义务罪】

(续上表)

《数据安全法》

第四章“数据安全保护义务”

第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第七章“附则”

第五十三条 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

《网络安全法》

第四章“网络信息安全”

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。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。任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息等。

《消费者权益保护法》

第二章“消费者的权利”

第十四条 消费者在购买、使用商品和接受服务时，享有人格尊严、民族风俗习惯得到尊重的权利，享有个人信息依法得到保护的权利。

第三章“经营者的义务”

第二十九条 经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。

经营者及其工作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。

经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。

(续上表)

《电子商务法》

第一章“总则”

第五条 电子商务经营者从事经营活动，应当遵循自愿、平等、公平、诚信的原则，遵守法律和商业道德，公平参与市场竞争，履行消费者权益保护、环境保护、知识产权保护、网络安全与个人信息保护等方面的义务，承担产品和服务质量责任，接受政府和社会的监督。

第二章“电子商务经营者”

规定电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定；明示用户信息查询、更正、删除以及用户注销的方式、程序，不得对用户信息查询、更正、删除以及用户注销设置不合理条件；有关主管部门应当采取必要措施保护电子商务经营者提供的数据信息的安全，并对其中的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供等。

第六章“法律责任”

第七十九条 电子商务经营者违反法律、行政法规有关个人信息保护的规定，或者不履行本法第三十条和有关法律、行政法规规定的网络安全保障义务的，依照《中华人民共和国网络安全法》等法律、行政法规的规定处罚。

第八十七条 依法负有电子商务监督管理职责的部门的工作人员，玩忽职守、滥用职权、徇私舞弊，或者泄露、出售或者非法向他人提供在履行职责中所知悉的个人信息、隐私和商业秘密的，依法追究法律责任。

《传染病防治法》

第八章“法律责任”

第六十八条（五）故意泄露传染病病人、病原携带者、疑似传染病病人、密切接触者涉及个人隐私的有关信息、资料的。

(续上表)

《妇女权益保障法》

第六章“人身权利”

第四十二条 妇女的名誉权、荣誉权、隐私权、肖像权等人格权受法律保护。

禁止用侮辱、诽谤等方式损害妇女的人格尊严。禁止通过大众传播媒介或者其他方式贬低损害妇女人格。未经本人同意，不得以营利为目的，通过广告、商标、展览橱窗、报纸、期刊、图书、音像制品、电子出版物、网络等形式使用妇女肖像。

《未成年人保护法》

第一章“总则”

第四条 保护未成年人，应当坚持最有利于未成年人的原则。处理涉及未成年人事项，应当符合下列要求：

(三) 保护未成年人隐私权和个人信息

第五章“网络保护”

第七十二条 信息处理者通过网络处理未成年人个人信息的，应当遵循合法、正当和必要的原则。处理不满十四周岁未成年人个人信息的，应当征得未成年人的父母或者其他监护人同意，但法律、行政法规另有规定的除外。

未成年人、父母或者其他监护人要求信息处理者更正、删除未成年人个人信息的，信息处理者应当及时采取措施予以更正、删除，但法律、行政法规另有规定的除外。

《邮政法》

第一章“总则”

第三条 公民的通信自由和通信秘密受法律保护。除因国家安全或者追查刑事犯罪的需要，由公安机关、国家安全机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。

(续上表)

《居民身份法》

第一章“总则”

第六条 居民身份证式样由国务院、公安部门制定。居民身份证由公安机关统一制作、发放。
居民身份证具备视读与机读两种功能，视读、机读的内容限于本法第三条第一款规定的项目。

第三章“使用和查验”

第十三条 公民从事有关活动，需要证明身份的，有权使用居民身份证证明身份，有关单位及其工作人员不得拒绝。
有关单位及其工作人员对履行职责或者提供服务过程中获得的居民身份证记载的公民个人信息，应当予以保密。

第四章“法律责任”

第十九条 国家机关或者金融、电信、交通、教育、医疗等单位的工作人员泄露在履行职责或者提供服务过程中获得的居民身份证记载的公民个人信息，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关处十日以上十五日以下拘留，并处五千元罚款，有违法所得的，没收违法所得。
第二十条 人民警察有下列行为之一的，根据情节轻重，依法给予行政处分；构成犯罪的，依法追究刑事责任：
(五) 泄露因制作、发放、查验、扣押居民身份证而知悉的公民个人信息，侵害公民合法权益的。

《统计法》

第一章“总则”

第九条 统计机构和统计人员对在统计工作中知悉的国家秘密、商业秘密和个人信息，应当予以保密。

第六章“法律责任”

第三十九条 县级以上人民政府统计机构或者有关部门有下列行为之一的，对直接负责的主管人员和其他直接责任人员由任免机关或者监察机关依法给予处分：
(二) 泄露统计调查对象的商业秘密、个人信息或者提供、泄露在统计调查中获得的可能识别或者推断单个统计调查对象身份的资料；
统计人员有前款所列行为之一的，依法给予处分。

参考资料

- ① 张新宝.从隐私到个人信息:利益再衡量的理论与制度安排[J].中国法学,2015(3):38-59.
- ② 袁纪辉.有关个人信息处理技术概念的厘清——匿名化、去标识化、假名化、去识别化之辨析[J].保密工作,2021(5):59-60.
- ③ 王俊.个人信息保护实践中落地难,专家呼吁加强国家规制 [EB/OL]. 2021[2021- 08- 23]. https://m.21jingji.com/article/20210525/herald/a906dad762096ff1c9d1b352a582f5e7_zaker.html.
- ④ 姚佳.论个人信息处理者的民事责任[J].清华法学,2021,15(03):41-54.
- ⑤ 张新宝.个人信息收集:告知同意原则适用的限制[J].比较法研究, 2019(6)
- ⑥ 全国人民代表大会常务委员会关于加强网络信息保护的決定:网络服务提供者收集公民个人电子信息时,应当明示收集、使用信息的目的、方式和范围,并经被收集者同意,不得违反法律、法规的规定。
- ⑦⑨ 韩旭至.个人信息保护中告知同意的困境与出路——兼论《个人信息保护法(草案)》相关条款[J].经贸法律评论,2021(01):47-59.
- ⑧⑬ 吕炳斌.个人信息保护的“同意”困境及其出路[J].法商研究,2021,38(02): 87-101.
- ⑩ 范为.大数据时代个人信息保护的路径重构[J].环球法律评论,2016,38(05):92-115.
- ⑪⑫ 郑佳宁.知情同意原则在信息采集中的适用与规则构建[J].东方法学,2020(02):198-208.
- ⑭⑰ 张凌寒.《个人信息保护法(草案)》中的平台算法问责制及其完善[J].经贸法律评论,2021(01):36-46.
- ⑮⑱ King & Wood Mallesons. 成年人要看的利弊——互联网数据商业化的模式变局 [EB/OL]. 2021[2021- 08- 23]. <https://www.chinalawinsight.com/2021/01/articles/compliance/%E6%88%90%E5%B9%B4%E4%BA%BA%E8%A6%81%E7%9C%8B%E7%9A%84%E5%88%A9%E5%BC%8A-%E4%BA%92%E8%81%94%E7%BD%91%E6%95%B0%E6%8D%AE%E5%95%86%E4%B8%9A%E5%8C%96%E7%9A%84%E6%A8%A1%E5%BC%8F%E5%8F%98/>

- ①②④杨婕. 中国信通院杨婕:《个人信息保护法》正式出台——中国走出第三条路 [EB/OL]. 2021[2021- 08- 23]. https://www.sohu.com/a/485071588_121181007
- ①⑨陈浩等. 个性化展示安全与合规报告(2020)[R]. 北京市环球律师事务所,南都个人信息保护研究中心,中国信息通信研究院安全研究所, 2020.
- ②⑩万方. 个人信息处理中的“同意”与“同意撤回”[J]. 中国法学,2021(01):167-188.
- ②⑪王俊. “个信法”二审:打出“连带责任+过错推定”组合拳,个人信息侵权诉讼将活跃 [EB/OL]. 2021[2021- 08- 23]. <http://www.sfccn.com/2021/4- 30/2NMDE0MDVfMTY0MTA2Nw.html>.
- ②⑫梅夏英. 论被遗忘权的法理定位与保护范围之限定[J]. 法律适用,2017(16):48-54.
- ②⑬杨子晔等. 协同构建保护个人信息删除权的治理体系[EB/OL]. 2021[2021-08-23]. https://www.thepaper.cn/newsDetail_forward_14105449.
- ②⑮程啸. 论个人信息处理者的告知义务[J/OL]. 上海政法学院学报(法治论丛):1-14[2021-08-20].

学术指导

周辉 中国社会科学院法学研究所副研究员，
中国法学会网络与信息法学研究会副秘书长

致谢

本报告筹备与撰写过程中得到了不少专家、学者支持，在此特别表示感谢。

王新锐 世辉律师事务所合伙人

邓志松 大成律师事务所高级合伙人

张仁卓 北京尚隐科技有限公司 CEO

何延哲 中国电子技术标准化研究院网安中心测评实验室副主任

夏海龙 上海申伦律师事务所律师

商希雪 中国政法大学网络法学研究所副所长

何兴驰 上海市锦天城(南京)律师事务所合伙人

监制:虞伟 曹金良

统筹:王俊 张雅婷

研究员/撰写:张雅婷 王俊 郭美婷

设计:林潢 徐晖 默默 邓居轩

2021年8月



南方财经全媒体集团合规科技研究院

关于个人信息保护的问题，您还关注哪些方面？

对我们的报告有什么意见与建议？欢迎沟通。

南方财经全媒体集团合规科技研究院研究员 张雅婷（zhangyt@21jingji.com）

南方财经全媒体集团合规科技研究院研究员 王俊（wangjun@21jingji.com）

南方财经全媒体集团合规科技研究院研究员 郭美婷（guomt@21jingji.com）