汉坤法律评述
2020 年 3 月 10 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

知识产权法律

2020 版《个人信息安全规范》重点解析

作者：段志超 | 蔡克蒙[1]

国家市场监督管理总局、国家标准化管理委员会于 2020 年 3 月 6 日正式发布了《信息安全技术 个人信息安全规范（GB/T 35273-2020）》（“**新版规范**”）。新版规范将于今年 10 月 1 日起正式生效，替代现行有效的《信息安全技术 个人信息安全规范（GB/T 35273-2017）》（“**旧版规范**”）。新版规范整体上延续了此前 2019 年 6 月和 10 月发布的两版《个人信息安全规范》征求意见稿的修改思路，系统地反映了监管部门近期对个人信息保护治理工作中提出的监管要求，针对个人信息收集不透明、强制和捆绑收集个人信息现象严重、个性化推送侵犯用户自主选择权、第三方隐秘收集信息缺乏控制、账号注销难、对生物识别信息的滥用和泄露频发等实践中个人信息保护疑难问题做出了有力回应。同时，我们也注意到新版规范相较旧版规范及此前征求意见稿在不少细节处进行了优化，更有助于合理开展个人信息保护工作。

本文尝试以问题为导向梳理和探讨新版规范的一些亮点，为企业合规提供概括性指南。

一、能读懂的通知 — 优化隐私设计提升透明度

自旧版规范实施以来，随着监管机构对隐私政策审查不断加强，很多企业的隐私政策已日趋规范，对个人信息处理情况做出了更加详实的披露，并为监管机构监督企业落实隐私的保护情况提供了有力的凭据。然而，隐私政策仍经常被批评篇幅冗长、晦涩难懂。新版规范优化了隐私政策的内容要求，并更加强调在隐私政策之外通过弹窗等交互界面实时告知用户，更有助于帮助用户理解个人信息处理情况，在知情基础上做出选择。

- 就形式而言，新版规范将“隐私政策”修改为“个人信息保护政策”[2]，意在明晰“隐私”和“个人信息”保护之间的区别，与《民法典（草案）》中对隐私和个人信息分别予以保护的思路保持一致。

[1] 实习生胡敏喆、周莎莎对本文的写作亦有贡献。

[2] 出于习惯考虑，本文仍沿用“隐私政策”这一惯用概念。

- 从隐私政策内容要求上看，新版规范与此前征求意见稿相同，删除了对披露个人信息控制者注册地址、常用办公地点、负责人联系方式（替换为控制者联系方式）、个人信息收集频率、存储地点、使用 Cookie、网站信标、像素标签等同类技术情况等过于法律或技术的事项。这将有助于缩减隐私政策篇幅，提升隐私政策可读性。

- 新版规范正式将此前征求意见稿提出的，且监管机构已通过《App 违法违规收集使用个人信息行为认定方法》等规范和执法实践提出的增强告知或实时告知要求纳入规范，包括个人敏感信息明确标识或突出显示，首次打开产品或服务、注册账号时通过弹窗展示隐私政策主要条款或核心内容，开启收集个人信息的扩展业务功能前通过弹窗等交互界面或设计告知功能所需个人信息等。这些增强告知的要求对企业产品的隐私设计提出了新的挑战。

二、分得开的同意 — 通过业务功能区分解决“最小必要”难题，强化用户控制力

如何落实数据收集的“必要性”和“最小化”原则是各国数据监管机构面临的共同挑战。这些原则在欧盟 GDPR 语境下被细化为三要素，即“充分性（adequate）”——个人信息足以实现处理目的，“相关性（relevance）”——个人信息与目的具有合理关联，“限于必要（limited to what is necessary）”——仅应收集完成目的所需的最少信息[3]。

然而，这些原则和设计要求仍过于抽象，在我国隐私保护理念方兴的环境中难以对业务实践提供具体指导。对此，新版规范承继了此前征求意见稿在区分业务功能的基础上界定信息收集范围的思路，禁止企业将基本功能与扩展功能捆绑，防止企业通过“功能捆绑”强迫个人信息主体接受个人信息收集。具体而言：

- 应当逐一告知用户扩展业务功能，逐项获得用户明示同意后开启；

- 用户拒绝开启扩展业务功能收集个人信息，企业不得拒绝提供基本业务功能或者降低服务质量，并且不得在 48 小时内再次征得用户同意；

- 用户有权关闭或退出业务功能，相应的途径或方式应与选择使用该项业务功能的途径或方式一样方便。

新版规范以业务功能为基础确定个人信息收集范围的要求，未来辅以关于相关常用服务类型最小信息的相关标准，对企业落实“最小必要”原则提供了具体的操作指引。企业在收集扩展功能对应的个人信息时，需要在其启动时逐项明示以获取用户的同意，实践中该操作可能会在用户体验和业务设计上给企业提出更多的挑战。此外，新版规范保留了此前征求意见稿“不应将改善服务质量、提升个人信息主体体验、研发新产品单独作为基本业务功能”的要求。这是否意味着企业需要开发允许用户自主选择的“用户体验计划”，方可收集改善服务、产品研发所需的个人信息，以及企业是否可以将基本业务功能收集的个人信息用于前述目的，是否需就此再次征得用户明示同意，仍有待通过监管要求和行业实践加以逐步明确。

三、特殊数据的特殊规则 — 新增生物识别信息处理严格限制

近年来，对生物识别信息，特别是人脸识别信息的过度收集、泄露和滥用引发的诸多伦理、隐私和安全

[3] 此外，欧盟数据保护机构还提出了数据避免（data avoidance，如果数据处理可能实现其他目的应避免进行个人数据处理活动）；聚合（aggregation，应当尽可能使用聚合性数据，避免对特定主体进行识别）；pseudonymization（如无需直接识别数据主体的个人数据，应对个人数据进行假名化处理，并单独存储识别密钥）；匿名化与删除（anonymization and deletion，如果个人数据对于目的的实现不再必要，应当对个人数据进行技术处理或从系统中去除有关个人数据，使得个人信息主体不再被识别或者关联）等原则。

问题在国内外均引起了广泛关注。欧盟委员会甚至曾提出了五年内禁用人脸识别技术的禁令[4]，尽管该禁令在发布不久后即被删除，但也足以反映其对人脸识别的高度关注和谨慎态度。而一直以隐私监管宽松而著称的美国，已有数州提出或通过关于人脸识别的立法，且有著名科技公司因为未经授权将面部识别数据用于用户标签建议被诉，最终承担数亿美金的赔偿金。我国近期发布的《个人金融信息保护技术规范》《人脸识别线下支付行业自律公约（试行）》均对人脸识别信息等生物识别信息的处理提出了严格规范。在此背景下，新版规范对个人生物识别信息的处理在生命周期各阶段提出了具体要求。

- **收集**：在收集个人生物识别信息前，应当单独向个人信息主体告知收集和使用生物识别信息的目的、方式和范围、存储时间等规则，取得个人信息主体明示同意。
- **传输**：应当采用加密等安全措施，如需采用密码技术宜遵循密码管理相关国家标准。
- **存储**：应当采用加密等安全措施，将个人生物识别信息与个人身份信息分开存储，原则上不应存储原始个人生物识别信息。
- **共享和转让**：原则上不应共享或转让个人生物识别信息，确需共享和转让的，仍应当单独向用户告知目的、信息类型等内容，并征得个人信息主体的明示同意。
- **披露**：不应公开披露个人生物识别信息。

前述合规要求对处理生物识别信息的技术公司构成了很大的合规挑战，这些公司往往不直接与客户交互，而仅向更“前端”的向用户提供服务的客户提供识别、验证服务，因此难以直接取得客户同意。提供生物识别信息识别和认证的企业需要与其客户共同制定或开发出符合新版规范要求的单独的信息采集或共享声明和同意方案。而对于在公共场所使用人脸识别系统用于人员分流、安全防护、甚至客流分析和个性化推荐等更难以取得明示同意的场景，如何落实新版规范的单独告知和同意要求则是相关企业亟需破解的合规难题。就现阶段而言，企业至少应按照规范要求，采取仅存储生物识别信息摘要信息，及时删除可提取个人生物识别信息的原始图像等措施，并在可能情况下尽可能实现在采集终端直接实现身份识别和认证功能。

四、打开的黑盒子 — 强化产品和服务提供者责任，约束第三方处理活动

第三方个人信息处理活动已经构成互联网产品生态的不可分割的环节。相比于个人信息控制者直接在提供产品或服务的过程中处理个人信息，第三方收集活动则较为隐蔽，用户无法追踪和感知信息的最终流向和使用目的。第三方采集的信息被用于与产品服务较为直接相关的场景，例如通过嵌入的 SDK 提供支付服务或地图服务，或用于对产品服务使用情况进行统计分析，进而基于用户行为向用户进行定向信息投放，甚至还可能被用于完全超出客户隐私预期的场景，例如用于信用评估。这些第三方应用的数据处理活动可能侵犯用户的知情权和自主选择权，并存在第三方借助网络产品或服务执行恶意操作，以及第三方数据泄露风险。鉴于此，我国监管机构此前征求意见稿中特别增加了关于“接入具备收集个人信息功能的第三方产品或服务”的规定，而去年出台的《App 违法违规收集使用个人信息行为认定方法》亦强化了直接向用户提供服务的互联网产品和服务个人信息控制者的责任，要求应当逐一列出委托的第三方或嵌入的第三方代码、插件等收集使用个人信息的目的、方式、范围。

新版规范延续了此前规定，从事前接入审查、告知同意、持续审计监管等维度全面加强产品和服务对接入或嵌入的第三方个人信息处理的监督审查责任。具体而言：

[4] https://www.telegraph.co.uk/news/2020/01/17/european-commission-mulls-ban-facial-recognition-technology/.

- **第三方接入前**：应当建立安全评估等机制，宜对第三方工具开展相关的技术检测；应当与第三方通过合同等形式明确双方安全责任，妥善留存合同与管理记录；
- **用户控制**：要求第三方自用户处获得收集个人信息的授权同意，并在必要情形中核验其实现的方式[5]。
- **第三方接入后**：向用户明确标识产品或服务由第三方提供，要求接入第三方建立个人权利响应机制并加强个人信息的安全管理。
- **发现未落实安全管理要求和责任时**：应当督促接入第三方及时整改，必要时及时停止接入。

此外，考虑到个人信息控制者权利和义务的平衡，相较此前的征求意见稿，新版规范删除了要求个人信息控制者“妥善留存、及时更新第三方权利响应机制”的要求，提出控制者仅在“必要情形下”对第三方获得用户授权同意的方式进行核验，一定程度上减轻了个人信息控制者的义务。

为了应对趋严的执法态势，企业需要对自身产品或服务中的第三方产品或服务进行详细摸排，及时删除或停止接入不必要或存在隐秘收集或滥用个人信息以及存在信息安全隐患的第三方产品或服务；若必须接入第三方产品或服务，应当向用户明确标识该产品或服务由第三方提供并详细披露第三方个人信息处理活动的具体情况。

五、多样选择 — 强化用户对个性化展示的控制力

个性化展示目前广泛应用于互联网广告、资讯推荐等领域。个性化推送在为用户节约搜索成本，更快地实现供需的匹配的同时，也引发对侵犯用户选择权，形成“信息茧房”，甚至是对数据主体造成歧视的担忧。

此次新版规范发布以前，多部法律法规已在这一方面做出了规范。例如 2019 年 1 月 1 日起实施的《电子商务法》要求电子商务经营者在根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项。2019 年 5 月发布的《数据安全管理办法（征求意见稿）》则规定，网络运营者利用用户数据和算法开展定向推送活动时，应当以明显方式标明“定推”字样，建立用户选择退出的机制并删除已经收集的设备识别码等用户数据和个人信息。

对此，新版规范继受了此前征求意见稿的规定，提升个性化展示的透明度和数据主体的控制力。

- 在向个人信息主体提供业务功能的过程中使用个性化展示，应显著区分个性化展示的内容和非个性化展示的内容；区分方式包括标明“个性化展示”或“定推”等字样，或区分栏目或版块进行展示；
- 在向个人信息主体提供电子商务服务的过程中，根据消费者的**兴趣爱好、消费习惯等特征**向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项；
- 在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应为个人信息主体提供简单直观的退出或关闭的选项并在用户选择退出后，向个人信息主体提供删除或匿名化有关信息的选项；
- 个人信息控制者还应当建立个人信息的自主控制机制，保障个人信息主体调控个性化展示相关程度的能力。

[5] 我们理解这一要求主要针对网页跳转、联合登陆等接入第三方服务场景，而对于第三方通过嵌入 SDK 等收集个人信息的，原则上应按照第 9.6 条由直接向用户提供网络产品或服务的个人信息控制者对用户进行告知并获得用户同意。

值得注意的是，新版规范认为，个人信息控制者基于用户选择的地理位置展示搜索结果的行为不属于个性化展示。究其原因，可能在于基于用户选择的地理位置进行展示是建立在用户选择基础上（例如在 OTA 服务中基于用户位置选择展示周边酒店），相对透明直观，用户对此具有控制力。基于同样理由，我们认为如基于用户设置的年龄、性别等其他基本特征向其展示内容或对搜索结果进行排序，不因个人信息主体身份而进行“千人千面”展示的，同样不应被视为个性化展示。

为了顺应上述监管要求，企业应积极在产品开发过程中重视对个性化展示的隐私设计，设置个性化展示的显著标识，设置关闭按钮或专门的隐私仪表板，允许用户对个性化展示进行控制。

六、迷宫不再 — 账户注销更加方便

强化个人信息主体权利保护，特别是注销账号权利的保护是监管机构近期的执法重点之一。去年 11 月，工信部开展信息通信领域 App 侵害用户权益专项整治行动，将“为用户账号注销设置障碍”列为一项重要的检查要点。根据工信部随后发布的两批侵害用户权益 App 名单和 App 专项治理工作组发布的《61 款 App 存在收集使用个人信息问题的通告》，先后有 60 余款 App 存在账号注销难的问题，包括规定了最短使用期限、需要用户提交身份证照片、手持身份证照片等条件。2019 年 12 月 30 日，国家网信办、工信部、公安部、市场监管总局还联合印发《App 违法违规收集使用个人信息行为认定方法》，再次重申，为注销用户账号设置不必要或不合理条件、未在 15 个工作日内响应用户权利的行为属于违法违规收集使用个人信息的行为。

在此背景下，新版规范首次将个人信息主体权利单独列为一章，并在此前征求意见稿基础上进一步细化了对个人信息主体注销账户权利的保护。

- 注销过程需要进行身份核验的，不应当提供多于注册、使用等服务环节收集的个人信息类型。如需注销核验过程需要收集个人敏感信息，应明确相关的处理措施，在达成目的后立即删除或做匿名化处理。
- 若多个产品或服务之间存在必要业务关联关系，而注销某个产品或服务的账户，会导致其他产品或服务的必要业务功能无法实现或者服务质量明显下降的，应向个人信息主体进行详细说明。
- 对于实践中“棘手”的多个产品或服务共用同一账号体系情况下的账号注销问题，新版规范规定企业可以将该产品或服务账号以外的信息做删除处理，及时切断账户体系与产品或服务的关联措施。
- 新版规范将此前征求意见稿的账号注销处理时限从十五天放宽至十五个工作日。

此外，值得注意的是，对于相应个人信息主体的请求，新版规范还建议企业直接在移动应用程序、网页、客户端软件中，设置便捷的交互式页面提供响应的功能或选项。此前，大量企业在实践中选择通过邮件、电话、客服聊天等人工方式响应个人信息主体的权利请求，而新版规范显然提出了更高的合规标准，便捷注销渠道的要求未来可能成为执法机关关注的重点。

七、结语

相较于《网络安全法》的提纲挈领，《个人信息安全规范》自实施以来即以其内容的丰富和可操作性引起实务界的瞩目，成为企业在个人信息保护实践中的重要指引以及相关监管机构执法的参照。同时，其非强制性国家标准的性质反而赋予了其在内容和尺度上的灵活性和开放性，既能响应数字化时代技术的快速迭代变革，着手解决新问题，又能兼顾隐私保护和企业实践的平衡，确保规则最终可以落地。

正基于此，我们预期《个人信息安全规范》的修订将是一个常规的过程，以期在充满不确定性和复杂性的数字时代背景下动态地寻找数据主体权利和数据流动效益之间的平衡。企业在密切关注规则变化，确保个人信息保护合规的同时，也应保持和监管部门的有效沟通，为合规实践中面临的问题寻找解决途径。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com

© 2020 Han Kun Law Offices. All Rights Reserved.