

October 14, 2022

To: Han Yi Clients and Friends

## 私域流量营销中的个人信息保护合规性初探

近年来，随着电信网络、物流、支付等基础设施与技术的进一步成熟以及疫情影响的进一步扩大，经济数字化得以持续推进。越来越多的品牌选择依托互联网与新媒体平台，寻求更高效的营销方式，与消费者建立更直接、更深度的联系，以进一步扩大其市场规模和品牌影响力。

在此需求的推动下，已有一定市场基础的 DTC（Direct To Customer /直接面对消费者）营销模式获得了进一步发展。很多品牌方不仅通过在大型电商平台开设店铺的方式吸引该等平台的注册用户与其发生交易，还试图将在该等电商平台上购买过其产品或服务的用户从平台这一“公域”进一步引流至品牌方建立的“私域”，形成品牌方自有的用户流量池，以便随时和反复接触和联系该等用户，提高用户对其产品或服务的复购率（“私域流量营销”）。目前常见的私域流量营销渠道包括微信社群、微信商城、企业微信、品牌 APP 或自建官网、社交媒体、短信或邮件等。在此过程中，品牌方不可避免地需要对平台用户的个人信息进行收集和使用，进而使得品牌方需要承担与该等个人信息收集、使用和保护相关的责任与义务。

本文将基于目前有关个人信息保护的监管现状及市场趋势，就品牌方企业在私域流量营销过程中可能涉及的、与消费者个人信息保护有关的主要法律问题及注意事项进行简要梳理和探讨，供有兴趣的朋友和相关企业参考。

### 一、 个人信息保护的监管现状与市场环境

1. 近年来有关个人信息保护的密集立法与强监管趋势对品牌方处理个人信息提出了更高的合规性要求。在法律法规层面，《民法典》及相关司法解释对自然人个人信息保护作出了原则性规定；《个人信息保护法》（“《个保法》”）及《信息安全技术 个人信息安全规范》（“《安全规范》”）、《互联网个人信息安全保护指南》等文件就个人信息保护建立了全生命周期管理体系；《消费者权益保护法》、《广告法》等规定对经营者收集、使用消费者个人信息做了规制；《电子商务法》、《网络交易监督管理办法》等规定了平台内经营者的消费者个人信息保护义务；《网络安全法》、《数据安全法》中对收集、使用数据（包括个人信息）提出了一般性要求；《刑法》及相关司法解释则对侵犯公民个人信息罪的界定与量刑等亦作出了规定。此外，汽车、医疗健康、金融领域等行业还制定了适用于该等领域的个人信息保护特别管理规定、安全指南和技术要求。

针对个人信息保护，以上法律法规、标准及指南等规则已经建立起了覆盖民事调整、行政监管和刑事制裁的全面网络，搭建起了以网络安全和信息化委员会办公室统筹协调，工业和信息化部、公安机关、市场监督管理局等政府部门多

元协同的联合监管框架，大大增强了对品牌方企业在私域流量营销过程中合规处理消费者个人信息的法律要求。

除逐渐完善立法以外，相关部门近年来也进一步强化了个人信息保护领域的执法与监管：如市场监督管理总局于 2019 年展开了“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动；工业和信息化部自 2019 年以来持续发布多批侵害用户权益行为的 APP 名单以及相关下架、整改通报；国家互联网信息办公室 2021 年以来对抖音、腾讯手机管家、Keep 等多款 APP 违法违规收集使用个人信息情况进行通报等。特别地，国家互联网信息办公室自 2021 年 7 月起对滴滴全球股份有限公司开展了持续一年的网络安全审查，并于 2022 年 7 月公示了其违法收集、处理个人信息、未尽个人信息处理告知义务等违法行为，并作出了人民币 80.26 亿元罚款等处罚决定，引发了广泛的社会关注。

2. 电商平台持续加强对用户个人信息的保护，增加了品牌方私域引流的难度。针对电商生态链路数据泄露、部分商户违规收集或使用消费者个人信息的情况频发、消费者投诉频繁等现象，为加强对平台用户的个人信息保护，顺应监管趋势，各大主要电商平台在对商户的管理层面以及技术层面陆续采取了相应措施以限制品牌方不当收集、使用平台用户个人信息。

近年来各大主要电商平台对其《商户入驻协议》、《隐私政策》等平台政策进行了持续的更新与修订，强化了对平台运营中涉及的用户个人信息的控制和保护。自 2021 年年初以来，一些电商平台陆续发布了系统升级改造方案（如淘宝的《订单处理类应用升级方案》、快手小店的《数据安全加密方案》、抖店的“消费者隐私数据加密项目”等），对平台用户的部分个人信息（如手机、电话、姓名及地址等）采取加密、脱敏等措施，使品牌方难以直接接触到用户的个人信息，增加了品牌方从平台获取用户个人信息的难度。

## 二、 私域流量营销过程中的个人信息保护：风险与应对

在日趋严格的个人信息保护监管环境和市场形势下，如何正确识别电商平台的用户个人信息，如何合法收集该等个人信息并用于品牌方的二次营销触达，如何在与第三方营销机构合作的过程中保护用户的个人信息安全等问题是品牌方企业在私域流量营销过程中所需关注的一些重点问题。

### 1. 正确识别“个人信息”

#### (1) 法律规定和司法实践

根据《个保法》，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。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”。<sup>1</sup>《民法典》、《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》还列举了一些典型的个人信息，包括姓名、出生日期、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况等。<sup>2</sup>

<sup>1</sup> 《个保法》第四条、第七十三条第（四）项。

<sup>2</sup> 《民法典》第一千零三十四条，《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第一条。

此外,《个保法》还将“一旦泄露或者非法使用,容易导致自然人的尊严受到侵害或者人身、财产安全受到危害的个人信息”列为“敏感个人信息”,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。对于敏感个人信息的收集与处理,需适用更严格的合规要求(如取得个人单独同意,事前进行个人信息保护影响评估并对处理情况进行记录等)。<sup>3</sup>

尽管《个保法》等相关法律规定已对“个人信息”进行了定义并有列举,但定义相对原则,且列举仅涵盖了典型情形。在司法实践中,除上述已明文列举的信息外,法院往往根据“可识别性”(即相关信息单独或结合其他信息是否可识别到个人)和“关联性”(即该信息是否为特定自然人在其活动中产生的信息)作为是否属于个人信息的判定原则,因此,淘宝账号、微信账号等互联网用户账号信息等在一定条件下也可能被认定为个人信息。

值得注意的是,相关信息即使经过加密、脱敏等措施处理,如仍能复原或与其他信息结合而识别到特定个人的,则不等同于“匿名化处理后的信息”,而仍属于个人信息的范畴。

鉴于我国有关个人信息保护的立法仍在不断发展和完善中,有关个人信息保护的执法也尚处在初级阶段,实践中对于某些具体的信息是否属于法律法规下规定的“个人信息”在认定上很多还处于模糊状态,如企业在涉及处理与自然人也有关的信息时,不能确定其是否属于匿名化处理后的个人信息的,从合规性角度出发,建议企业及时就该等信息的性质咨询相关主管部门。

## (2) 识别从电商平台获取的个人信息

品牌方在电商平台上运营店铺、销售商品或服务的,为了实现交易、提供配送和售后服务之目的,目前能够从电商平台上获取的与消费者相关的信息主要包括(不同平台获取的信息范围不完全相同):用户账户名、姓名、性别、所在省市、历史交易及特定交易记录、商品/服务信息、收件人姓名、地址、联系方式、物流跟踪信息、支付信息等,其中,有些平台共享给品牌方的用户姓名、电话号码、地址是部分文字、数字被隐藏的脱敏或加密信息(如将姓名脱敏显示为张\*甲)。

为避免合规风险,品牌方拟将在电商平台上获取的用户信息用于私域流量营销的,应首先了解和识别其从电商平台获取的与消费者有关的信息中哪些属于个人信息和敏感个人信息,并在后续披露和使用过程中注意对用户个人信息的保护。

根据上文介绍的法律法规和一般理解,在品牌方从平台上获取的与消费者有关的信息中,收件人姓名、地址、联系方式通常会被认定为是典型的用户个人信息;用户所在省市、性别、用户账户名等信息与其他信息结合时能识别到特定个人的,也可能被认定为个人信息;交易记录、支付信息、交易商品/服务信息因涉及个人宗教信仰、医疗健康、金融账户、行踪轨迹等信息的,可能被认定为消费者的“敏感个人信息”。对于品牌方在店铺运营中自平台取得的加密或脱敏后的用户信息,由于实践中往往也能被复原或与其他信息结合而能识别到特定个人,因此一般也属于个人信息。

---

<sup>3</sup> 《个保法》第二十八条、第二十九条、第五十五条第(一)项。

## 2. 合法收集个人信息

### (1) 主要法律要求

根据《安全规范》，<sup>4</sup>个人信息的“收集”是指获得个人信息的控制权的行为，包括：(i)由个人信息主体主动提供、(ii)通过与个人信息主体交互或记录个人信息主体行为等自动采集行为，以及(iii)通过共享、转让、搜集公开信息等间接获取个人信息等行为。根据《个保法》，个人信息的收集属于个人信息的处理，应当遵循合法、正当、必要和诚信等原则和规则，其中主要包括：<sup>5</sup>

- 目的明确和最小必要原则：处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关并限于最小范围，还应当采取对个人权益影响最小的方式。
- 公开处理信息并有效告知：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：(i)个人信息处理者的名称或者姓名和联系方式；(ii)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；(iii)个人行使法定权利的方式和程序；及(iv)法律、行政法规规定应当告知的其他事项。如有相关事项发生变更的，还应当将变更部分告知个人。
- 取得个人信息主体的同意：除法定无需取得个人同意的情形外，<sup>6</sup>用户需在其充分知情的前提下自愿、明确作出同意，如主动点击“同意”“注册”“发送”“拨打”、主动填写或提供信息等。

此外，《个保法》还要求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的，接收方应当在提供方告知的处理目的、处理方式和个人信息的种类等范围内处理个人信息；如接收方变更原先的处理目的、处理方式的，应当重新取得个人同意。<sup>7</sup>

### (2) 平台政策要求

在目前的电商平台交易惯例中，针对普通商户，电商平台通常会在《商家入驻协议》、《隐私政策》等平台政策中规定，为实现平台内交易、提供该等交易的配送和售后服务之目的，平台将向品牌方共享平台用户的部分个人信息（主要包括收件人姓名、电话号码、地址等，其中部分为脱敏后的信息）；对于该等用户个人信息，品牌方仅能为上述目的而收集和使用。如品牌方获得用户个人

---

<sup>4</sup> 《安全规范》3.5。

<sup>5</sup> 《个保法》第五条到第七条、第十三条、第十七条。

<sup>6</sup> 《个保法》第十三条：“符合下列情形之一的，个人信息处理者方可处理个人信息：……（二）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；（三）为履行法定职责或者法定义务所必需；（四）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；（五）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；（六）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；（七）法律、行政法规规定的其他情形。依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。”

<sup>7</sup> 《个保法》第二十三条。

信息的实际不仅仅在于实施平台内交易及提供相关配送、售后服务，还在于引流并对用户反复触达营销的，由于品牌方变更了个人信息处理目的，不仅可能涉及到违反平台政策的规定，需对平台承担相关违约责任（如扣除保证金、支付违约金、被封禁商品、关闭店铺、删除且不再收集使用相关数据等），同时还可能构成了违规收集消费者个人信息，需承担相应的法律责任。

而对于开通了一些平台提供的品牌会员功能（如“店铺会员”、“品牌会员”、“会员通”等）的品牌方，平台通常允许品牌方邀请购买过品牌商品或服务的平台用户在平台内注册成为品牌方会员，并超越“平台交易、配送和售后”之目的收集已加入会员的平台用户的个人信息，以及通过平台允许的特定渠道（如短信、客服消息等）向已成为品牌方会员的消费者反复发送与品牌产品或服务相关的商业性信息（如品牌产品推荐、广告促销信息、品牌资讯等）。

### **(3) 品牌方从电商平台收集个人信息的注意事项**

如前所述，由于品牌方通过电商平台间接获取了消费者的个人信息，根据相关规定和一般理解，品牌方的行为构成对用户个人信息的收集和使用，需要遵守个人信息处理的法定要求和相关平台政策的规定。

#### **(a) 需重新取得消费者的个人同意**

对于一般的品牌方而言，如品牌方希望利用从平台获得的用户信息将平台上接触到的客户作为其私域流量营销的对象，由于其从电商平台获取消费者个人信息的目的实际发生了变更（从实现平台上的交易、提供配送和售后服务之初始目的，进一步扩大至引流后的反复触达营销之目的），根据相关规定，品牌方需要就其对消费者的个人信息收集行为重新或另行单独取得消费者的同意，否则，可能会构成违规收集消费者个人信息，需因此承担相应的法律责任。

为重新或另行单独取得消费者的同意，品牌方可以考虑开通平台提供的会员功能。在邀请已在平台店铺购买过其商品或服务的存量用户成为品牌会员时，品牌方可通过会员协议、隐私政策等方式向用户直接告知其个人信息处理目的与方式的变更，并通过用户主动勾选“同意”等方式获得其授权同意，以允许品牌方通过短信、电话等形式向其发送品牌产品推荐、广告促销、品牌资讯等商业性信息。<sup>8</sup>

如平台无会员功能或品牌方未开通该等功能的，品牌方可考虑采取其他方式获得存量用户对其反复触达营销的授权同意。如在向用户寄送其在平台购买的产品的同时附赠优惠卡片邀请用户添加品牌方的微信小程序、企业微信或社群，品牌方可通过小程序、卡片标注等方式，充分告知用户其收集信息的类型、收集目的、处理方式等事项，并在最小必要范围内收集其个人信息。在用户了解该等事项后，主动扫码添加小程序、企业微信、进

---

<sup>8</sup> 如天猫 OralB 欧乐 B 官方旗舰店的品牌会员页面所载，根据《宝洁品牌会员服务协议》与《隐私协议》：您注册本店铺会员，视为您同意宝洁通过本店铺收集、使用您的个人信息，包括……；您同意，我们将您的上述个人信息用于以下目的和用途：（1）履行订单；（2）整合分析以了解和评估细分消费群体的兴趣、要求和需求，以开发并改进我们的产品和服务；（3）为您提供或寄送个性化的产品、产品介绍、活动礼品和宝洁品牌产品推荐；以及（4）为您推送个性化的品牌资讯、广告和促销信息。我们可能会不定期通过包括电子邮件、短信、品牌社交媒体账号、天猫客服消息、旺旺、支付宝服务等方式向您推送与上述目的相关的信息。

入社群等行为可视为品牌方取得了消费者同意。

### **(b) 需获得平台的授权**

如前所述，实践中，一些电商平台通常会在平台政策中要求，品牌方只能为提供平台政策约定范围内的交易和提供配送、售后服务目的而收集和使用权平台用户的个人信息。

对于提供品牌会员功能的平台，品牌方需要满足平台对于开通该等功能商户的要求，并在该等服务功能允许的个人信息处理目的、方式及范围内进行私域流量营销。若平台无此服务或品牌方未能开通该等服务功能的，如上文介绍的，品牌方应在遵守平台有关规定的前提下，通过合法渠道和方式自行取得相关用户的单独同意，为私域流量营销之目的，收集并使用平台用户信息。

## **3. 合法使用个人信息**

### **(1) 法律规定**

根据《个保法》的相关规定，对个人信息的“使用”属于对个人信息的“处理”，同样应当符合合法、正当、必要等个人信息处理原则，告知用户使用其个人信息的规则并在其授权同意的范围内进行使用。并且，个人信息处理者还应当保障其个人信息权益的行使，需向用户提供便捷的同意撤回方式；个人撤回授权同意后，个人信息处理者后续不应再处理相应的个人信息。<sup>9</sup>

此外，若个人信息处理者与第三方进行数据合作处理或需要与第三方交互个人信息的，不同的合作形式适用不同的法律关系及权利义务规定。在私域流量营销的场景中，部分品牌方囿于人员配置、技术能力等多方面的限制，经常需要委托第三方利用品牌方获取的消费者个人信息开展营销推广活动。鉴于品牌方是个人信息的收集和使用方，其对该等个人信息的使用和保护合规性和适当性承担最终的责任，因此，在委托第三方处理个人信息的过程中，品牌方应特别注意在委托合作协议中规范、限制和监督第三方对于该等个人信息的处理和责任，以防止个人信息的不当使用和泄露。<sup>10</sup>

### **(2) 使用个人信息的注意事项**

#### **(a) 注意平台政策中的使用限制**

如前所述，电商平台往往会对品牌方披露和使用通过平台获取的用户个人信息等行为进行限制。如有些平台协议会要求品牌方不得对平台上的数据（包括用户个人信息）进行商业性利用，也不得将其基于平台获知、收集的用户个人信息披露给第三方；有些商家入驻协议中要求品牌方在无用户另外授权的情况下，不得将店铺经营过程中收集、使用、共享的用户个人信息用于平

<sup>9</sup> 《个保法》第四条、第十五条、第四十四条、第四十七条、第五十条；《安全规范》8.4。

<sup>10</sup> 根据《个保法》第二十一条、第五十五条等相关规定，在个人信息的委托处理中，受托方需根据委托方委托在约定范围内处理个人信息，委托方需要对受托方在委托合同约定范围内的处理活动负责。委托人应与受托方签署委托合同，约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，在事前进行个人信息保护影响评估并对受托方的个人信息处理活动进行监督。

台交易之外的目的；否则品牌方需承担扣除保证金、支付违约金、查封账户、删除且不再收集使用相关数据等违约责任。

对于平台政策中的披露和使用限制，品牌方可以考虑通过平台提供的会员功能或取得平台授权同意后，在相关平台政策允许的范围内、及用户授权同意的前提下，对用户进行私域流量营销。

### (b) 约束合作方行为

品牌方委托合作方使用存量用户的个人信息进行私域流量营销的，品牌方通常需要将用户的相关个人信息披露给合作方。为保护用户的个人信息安全，降低合规风险，品牌方应尽量缩小用户个人信息披露的范围，并通过合同约定及监督等方式约束第三方使用用户个人信息的行为。具体而言：

- 告知用户个人信息委托处理的情况、保证个人在个人信息处理活动中的主体权利：在委托处理的场景下，现行法律要求将委托处理方式告知用户，但对是否需取得用户的授权同意规定不明确，实践中存在不同理解。为避免可能的风险和纠纷，建议品牌方将委托第三方处理个人信息的处理方式告知用户并尽量获得同意。特别地，品牌方应当保障用户的个人信息主体权益，提供修改、删除其个人信息的渠道及便捷的撤回同意的方式；在用户撤回同意后，不再继续向其发送商业营销类信息；同时建立个人行使权利的申请受理和处理机制，为其提供便捷有效的行权途径。
- 事前就委托行为进行个人信息安全影响评估并对处理情况进行记录：品牌方应当对拟合作的第三方服务机构进行全面完整的尽调，确保其具有适当的数据安全能力，并参照《个保法》、《信息安全技术 个人信息安全影响评估指南》等规则进行个人信息安全影响评估。
- 与受托方签署委托合同：在委托合同中明确双方权利义务，约定受托方处理个人信息的范围、处理目的、处理方式等，并限制或禁止受托方转委托他人处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托方应当将个人信息返还个人信息处理者或者予以删除，不得保留。此外，品牌方还应当重视合同中受托方的合规承诺保证、个人信息数据保护义务及信息安全措施等条款。
- 对受托方的个人信息处理活动进行监督：品牌方可考虑设置随时对受托方开展进场或书面检查的权利，以确保受托方具有数据安全管理和安全技术保障能力；同时要求受托方在产生可能影响委托协议的履行的情形发生时向品牌方进行告知并保留品牌方单方解约、要求赔偿等权利。

对于经营中涉及用户个人信息的企业来说，除上述提到的应当在收集、使用环节注意合规性之外，还应当在储存、加工、传输、公开、删除等其他处理环节以及日常合规管理中制定和履行内部个人信息管理制度和操作规程，对个人信息实行分类管理，采取相应的加密、去标识化等安全技术措施，合理确定从业人员个人信息处理操作权限并定期进行安全教育和培训，制定并组织实施个人信息安全事件应急预案等，<sup>11</sup>以确保个人信息处理活动符合法律法规的规定，防止个人信息泄露。

---

<sup>11</sup> 《个保法》第五十一条。

此外，值得注意的是，根据相关规定，处理个人信息达到 100 万人的企业在数据收集、使用、存储、出境等方面还需要遵守比一般数据处理者更高的要求，如需向境外提供个人信息的，应当向网信部门申报数据出境安全评估；有赴国外上市计划的，还需要依法向网络安全审查办公室申报网络安全审查等。<sup>12</sup>

### 三、 小结

在数字经济时代，为应对个人信息保护和数据安全方面全新的法律秩序与市场环境，品牌方企业应当在正确识别消费者个人信息的基础上，在收集、使用（包括委托第三方处理）消费者个人信息的各个环节、日常经营、融资上市及其他活动过程中严格保护消费者的个人信息和维护自身的数据安全。

© 2022 年 10 月 瀚一律师事务所

---

<sup>12</sup> 《个保法》第四十条；《网络数据安全条例（征求意见稿）》第五条、第十三条。有兴趣的人士可参考我所于 2021 年 11 月 17 日发布的客户通讯《<网络数据安全条例（征求意见稿）>速评 —— 网络数据安全迎来强监管时代》。