

[illegible]

对于与用户权益存在重大关系的条款，隐私政策中通常会以显眼的标注方式（加粗、斜体和下划线等）来提示用户对此类重点条款予以特别关注。通过对样本APP隐私政策进行总结，并结合团队实务经验，我们归纳出以下四类高频出现的重点条款：

我们整理归纳发现，15个样本APP隐私政策中均包含未成年人隐私条款。然而，关于其中获取监护人同意的规定，微信的要求是最严格的之一，其明确要求18周岁以下的未成年人需取得监护人的“书面同意”。QQ音乐要求较为宽松，其允许已满14周岁未满18周岁的未成年人，自行授权同意隐私政策。

对未成年人中未满14周岁的儿童，有11个样本APP制定了专门的儿童隐私保护规则。虽然《个保法》并未明确“专门的个人信息处理规则”是否需要以单独文件的形式体现，但结合上述样本APP的实践，对于用户可能或者确定涉及未满14周岁儿童的公司，除隐私政策以外，我们建议制定单独的儿童隐私保护规则，以备符合日趋严格的监管要求。

1.2 生物识别信息处理条款

根据《信息安全技术个人信息安全规范》（GB/T 35273-

2020），生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。由于生物识别信息属于个人信息中的敏感个人信息，其具有区别于其他个人信息的法定要求。根据《个保法》，处理敏感个人信息应当取得个人的单独同意，且应告知处理敏感个人信息的必要性以及对个人权益的影响。

我们通过梳理归纳，将样本的隐私政策APP中涉及生物识别信息的具体功能可分为：面部美化功能、验证和登录功能（不含实名/实人认证）

和其他功能。这些功能主要涉及的生物识别信息为指纹、声纹和面部识别特征。实现面部美化功能是部分样本APP处理生物识别信息的常见场景之一。对于用户生物识别信息，采取在用户本地设备中而并不上传至服务器是较为通常的做法，或者上传至服务器但同时做去标识化处理/匿名化处理，这在一定程度上减轻或规避了公司处理生物识别信息可能需要面临的风险。

1.3 实名/实人认证条款

实名/实人认证条款主要由个人信息类型和使用场景组成。各样本APP中实名/实人认证条款主要收集的个人信息是姓名、身份证号码和面部信息，其次还有手机号和银行卡信息。因而，公司需根据收集的具体个人信息类型判断其是否涉及敏感个人信息，并相应地对其中的敏感个人信息履行法定义务。

经梳理15个样本APP隐私政策，实名/实人认证的主要场景包括：账号注册、使用第三方帐号登录时的内容发布和进行直播。除了个人信息类型和使用场景，个别APP会具体说明认证的方式（自主认证、借助第三方、人工认证），以及第三方的信息处理方式和认证完成后信息的处理（存储或删除）。腾讯会议的直播功能中直播方需要进行实人认证，但不存储相关信息。淘宝的部分功能涉及实名/实人认证，其表示将存储认证信息及认证结果。但存储认证信息的APP表示存储仅用作认证用途，不会超范围使用。

1.4 自动化决策条款

自动化决策是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行

决策的活动。通过分析样本APP的隐私政策我们发现：自动化决策条款主要由收集的个人信息类型、用户对自动化决策的管理和信息处理方式组成。

15个样本APP的隐私政策中通常通过向用户说明如何管理和关闭相应个性化功能，来履行《个保法》限制信息推送和商业营销的要求。此外，由于个性化决策基于APP收集的各类信息，因而删除此类信息也是管理个性化决策活动的一种方式，从而通过限制个人信息来源的方式达到限制效果。

综上所述，我们理解，隐私政策没有所谓的标准模板，而是应结合公司自身业务实际情况，综合考虑个人信息类型的广度，处理个人信息的方式和履行法定义务的合规程度，来制定和更新适宜公司的隐私政策。

二、APP隐私政策的重点条款分析

在本文的第二部分，我们按照

“商务”、“购物”、“社交”、“金融财务”、“娱乐”、“音乐”和“摄影”的分类，对样本APP进行隐私政策特点的分析。

2.1 商务类APP

商务类APP通常会针对个人用户、企业用户、最终用户进行场景的分别阐述。并根据产品的定位，加入面向目标用户群体的个人信息收集模块。并且，为了提升用户体验以及更好的满足办公功能，商务类APP通常会与其他办公功能进行衔接。同时，由于商务类APP涉及到的企业敏感信息较多，如何处理信息留存期限成为商务类APP的一个必须要考虑的问题。在这方面，商务类APP或许会选择给予企业用户一些自主权限。

2.2 购物类APP

由于购物类APP需要吸引、引导用户的购买欲望并满足用户的购物需求，购物类APP一般会较为注重信息推送和商业营销，通过收集信息来完成自动化决策。所以，如何使得其自动化决策满足日渐收拢的信息保护监管要求成为购物APP的一个关注要点。并且，购物类APP还会基于对整个平台用户的浏览、搜索、热点进行推荐分析，并形成精选榜单单向用户推送。最后

，因为购物类APP在支付与配送方面（核心功能）一般与第三方机构进行合作，需要将用户订单信息与第三方共享，购物类APP在撰写其隐私政策时，一般会关注如何与第三方隐私政策做出切割。

2.3 社交类APP

为了实现互动功能，社交类APP的特色是一般会给予用户对于APP所收集的信息是否向外界公开、公开的内容一定的自主权限，并根据用户的需求设置收集信息的范围。

2.4 金融财务类APP

如果用户想要正常使用金融财务类APP的核心功能，需要提交的必备信息范围较大、且属于敏感信息。所以，如何实现满足金融监管要求与个人信息保护之间的平衡是金融财务类APP的关注要点之一。并且，金融财务类APP需要谨慎处理其与第三方服务之间的责任切割，着重关注信息共享、风险隔离的措施与条款。

2.5 娱乐类APP

娱乐类APP需要收集的必备信息较少，但是如果涉及到直播开播、资金流动等特殊活动，可能会要求用户进行实名认证。并且，娱乐类APP在定向推荐与用户画像条款的设置上，也有其自身特点，一般是依据该娱乐类APP的定位，推送音视频内容、资讯，而不完全是商业类广告。

2.6 音乐类APP

为了使用户更好地使用音乐类APP的产品或信息，在某些特殊场景下，如申请特殊身份或职业认证，音乐类APP会收集用户的声纹信息，以完成审核。所以，如何收集、使用该等较为特殊的个人生物识别信息成为了音乐类APP的关注要点之一。

2.7 摄影类APP

为了实现某些特殊功能，摄影类APP普遍需要面部识别信息。摄影类APP应采取向用户明确告知、列举收集信息的范围、内容、目的，并以去标识、匿名化处理等各种方式处理面部识别信息，以减轻面临的合规风险。

综上所述，APP的运营者应当关注个人信息保护领域的监管要求所涉及的重点条款，并根据自身行业特色对用户协议及隐私政策的内容进行合规调整以及减少风险。

作者



潘尤迪
权益合伙人
上海
+86 21 6105 0917

apan@yuandawinston.com



毛雨媛
律师
上海
+86 21 6105 0572

kamao@yuandawinston.com