**附件2**

**重点整治问题的典型违规场景**

**一、扰乱竞争秩序方面**

**（一）“恶意对其他互联网企业服务或产品的网址链接实施屏蔽等不兼容行为”**

典型场景1：具有外部网址访问功能的即时通信软件，无正当理由限制其他互联网企业服务或产品的网址链接的识别、解析、正常访问。

典型场景2：具有信息发布功能的应用软件，无正当理由对具有相同条件的其他互联网企业服务或产品的网址链接实施歧视性屏蔽措施。

**（二）“妨碍、破坏其他互联网企业服务或产品的正常安装、运行等恶意干扰行为”**

典型场景1：在互联网企业服务或产品安装、升级过程中，通过弹窗提示，附加不必要的操作步骤等方式误导用户使用其他应用分发平台安装、升级。

典型场景2：擅自关闭其他互联网企业服务或产品正常运行的必要权限，导致部分功能无法正常使用。

**二、侵害用户权益方面**

**（三）“移动智能终端应用软件启动弹窗信息页面未提供显著，有效的关闭或跳过功能，或利用文字、图片、视频等方式欺骗误导用户跳转至其他页面”**

典型场景1：APP启动时，开屏弹窗信息页面未提供关闭／跳过按钮，或者按钮过小或非常隐蔽，导致用户找不到或者弹窗信息关不掉，无法正常进入使用界面。

典型场景2：APP启动时，开屏弹窗信息页面使用整屏图片作为跳转链接，或采用欺骗诱导性文字描述，导致用户在非知情自愿的情况下，碰触页面任意区域都跳转至其他页面或下载其他应用程序。

**（四）“未征得用户同意向第三方提供用户个人信息，或未向用户明确列出第三方主体身份信息、处理目的、处理方式及个人信息种类等；提供个性化推荐服务时，未提供显著、便捷、有效的关闭个性化推荐服务的选项”**

典型场景1：APP未征求用户同意，或仅在用户隐私协议中以格式条款的形式强迫用户同意向第三方提供用户个人信息，且未详细列明第三方的主体身份信息、处理方式及个人信息种类等。

典型场景2：APP的定向推送功能未对用户提供关闭此功能的选项，或者提供虚假的关闭选项。

**三、威胁数据安全方面**

**（五）“在用户数据收集，传输、存储等环节，未按法律法规要求建立数据安全管理制度和采取必要的安全技术措施”**

典型场景1：企业尚未制定数据全生命周期安全保护制度，未明确数据分类分级，权限管理，监测巡查、应急管理、投诉处理等操作规程和要求。

典型场景2：企业收集的用户数据未采取数据分类、重要数据备份等措施。

典型场景3：企业相关涉数据存储系统中未对用户身份信息等敏感数据进行加密存储、未采取访问和权限控制措施。

典型场景4：在网站或移动应用程序前后端数据传输过程中，未对用户身份证号、用户鉴权信息等敏感数据进行加密或未使用安全的传输协议。

**（六）“在向第三方提供用户数据时，未按法律法规要求采取安全评估、日志审计等必要的技术和管理措施”**

典型场景1：具有用户信息验证、营销活动推广等跨平台用户数据提供场景的业务，企业未在提供数据前征得用户明示同意。

典型场景2：在向第三方提供用户数据前，未对第三方数据保护制度和技术能力情况进行安全评估；或在数据提供过程中，未开展保护能力有效性持续监督验证。

典型场景3：在向第三方提供用户数据过程中，未定期对企业与第三方的数据共享接口进行安全审计，不掌握数据实际提供量级与类型等情况。

**四、违反资质和资源管理规定方面**

**（七）“违规建设经营通信传输设施等无证经营、超范围经营基础电信业务；使用无相应电信业务经营许可的主体提供的通信传输设施服务和带宽、电路等网络接入资源；违反电信业务经营许可相关规定和守法合规经营承诺”**

典型场景1：未获得基础电信业务经营许可，擅自建设经营通信传输设施。

典型场景2：未按电信业务经营许可证载明的电信业务种类，在规定业务范围内经营电信业务，超业务经营范围和地域范围经营相关电信业务。

典型场景3：从事业务经营活动，使用未取得相应电信业务经营许可证的主体提供的网络基础设施和带宽、电路等网络接入资源。

典型场景4：向其他从事接入服务的增值电信业务经营者转租所获得的带宽等网络接入资源。

**（八）“互联网协议地址、域名等资源使用方式不符合电信管理机构有关规定；未切实履行非经营性互联网信息服务备案、及时更新备案信息等要求”**

典型场景1：互联网信息服务提供者使用的互联网协议地址未按要求履行备案手续，或备案信息变更后未在规定时间内更新。

典型场景2：互联网信息服务提供者使用的域名未备案，或履行备案手续后，域名过期未及时注销备案，擅自进行域名转让，违规变更域名注册服务机构等。

典型场景3：未备案即从事非经营性互联网信息服务，或未及时更新备案信息。