网络安全及数据合规动态（2020 年 1 月-6 月）：监管规则（上）

作者：傅鹏、赵卿梦、俞沁

前言：

2020 年上半年，在我国网络安全与数据合规监管实践发展的进程中，是具有里程碑意义的一个时间段。

受新冠疫情影响，许多行业的业务形态和工作方式的“线上化”加速。随着“新基建”等系列政策的颁布，5G、人工智能、工业互联网、物联网等领域的发展享受政策利好。

受上述因素影响，诸多业态对个人信息和其他数据的收集和利用频率空前频繁、程度不断加深，数据流转需求显著放大。“数据经济”的价值进一步释放。

在此背景下，擅自收集、滥用个人信息的情况也更加普遍，监管需求增大，实际的监管活动不断加码，适应“数据经济”快速发展的全新监管规则频出。

我们利用两篇推送文章的篇幅，对 2020 年上半年网络安全及数据合规领域的监管新规进行总结；利用一篇推送文章的篇幅，对 2020 年上半年网络安全及数据合规领域引人关注的部分事件进行分析。

本动态是 2020 年 1 月至 6 月网络安全和数据合规的最新监管规则简述的上篇，主要对 App 场景下的个人信息保护规则以及综合性个人信息监管规则进行介绍和简述。

我们的下一期动态，将展现 2020 年 1 月至 6 月网络安全和数据合规的最新监管规则简述的下篇，主要介绍行业细分领域下的个人信息与网络安全保护规则，包括教育、电商、金融、工业等领域。

本动态仅作为本所对网络安全及数据合规相关的近期话题的一般性探讨，不构成本所正式法律咨询意见。

- **监管规则目录**：

发布时间	规则名称	发布单位
App 场景下的个人信息保护规则		
2020.01	《信息安全技术 移动互联网应用（App）收集个人信息基本规范（征求意见稿）》	全国信息安全标准化技术委员会
2020.03	《网络安全标准 2020 自评估指南—移动互联网应用程序（App）收集使用个人信息自评估指南(征求意见稿)》	全国信息安全标准化技术委员会
2020.03	《App 个人信息安全防范指引（征求意见稿）》	全国信息安全标准化技术委员会
个人信息的综合性监管规则		
2020.01	《信息安全技术 个人信息告知同意指南（征求意见稿）》	全国信息安全标准化技术委员会
2020.03	《信息安全技术 - 个人信息安全规范》	国家市场监督管理总局、国家标准化管理委员会
2020.05	《中华人民共和国民法典》	全国人民代表大会
2020.06	《浙江省公共数据开放与安全管理暂行办法》	浙江省人民政府

一、 App 场景下的个人信息保护规则

(一) 《信息安全技术 移动互联网应用（App）收集个人信息基本规范（征求意见稿）》

全国信息安全标准化技术委员会（“**信安标委**”）于 2020 年 1 月 20 日发布了《信息安全技术 移动互联网应用（App）收集个人信息基本规范（征求意见稿）》（“**《App 个人信息收集规范》**”），对此前国家市场监督管理总局及国家标准化管理委员会于 2019 年 10 月 24 日联合发布的《信息安全技术 移动互联网应用程序(App)收集个人信息基本规范(草案)》(“**2019 年《App 个人信息收集规范》草案**”）进行了修订。其中，特别值得关注的是：

(1) 个人信息共享和转让规定的变化

2019 年《App 个人信息收集规范》草案中规定，存在共享、转让个人信息的情况下 ,App 运营者应向个人信息主体提供实时查询数据接收方身份的途径；《App 个人信息收集规范》删去了对 App 运营者的前述规定。但与此同时，《App 个人信息收集规范》要求，通过间接方式收集个人信息的，App 运营者应向个人信息主体提供实时查询数据提供方身份的途径。

由此可见，在存在个人信息共享和转让的情况下，向个人信息主体提供查询途径，从数据提供方的义务转换为了数据接收方的义务，即数据提供方无需向用户提供查询其数据对外共享的情况，但是如果数据接收方从第三方处获得用户的个人信息，其应对用户提供查询途径，查询个人信息来源。

(2) 明确常见服务类型中收集的、作为最小必要信息的“网络日志”内容

根据《网络安全法》第 21 条的规定，网络运营者应当采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月，在 2019 年《App 个人信息收集规范》草案中亦基于这一依据，规定在地图导航、网络约车、即时通讯等服务类型需收集的最小必要信息中包含“网络日志”，但是未明确此处“网络日志”的具体内容和范围。

在《App 个人信息收集规范》中，“网络日志”被限制在“网络访问日志”范围内，并且明确规定该等信息的收集仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要，该等“网络访问日志”信息通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。

(3) 新增了常见服务类型及相关的最小必要信息

《App 个人信息收集规范》增加了 9 种常见服务类型，并就每一服务类型下最小必要信息作出规定，具体包括：旅游服务、酒店服务、网络游戏、在线影音、儿童教育、电子图书、拍摄美化、应用商店和网络直播。

(二) 《网络安全标准 2020 自评估指南—移动互联网应用程序（App）收集使用个人信息自评估指南(征求意见稿)》

信安标委于 2020 年 3 月 19 日发布了《网络安全标准 2020 自评估指南—移动互联网应用程序（App）收集使用个人信息自评估指南(征求意见稿)》（“**2020 版自评指南**”）。在形式上，2020 版自评指南基本延用 App 违法违规收集使用个人信息专项治理工作组于 2019 年 3 月 1 日发布的《App 违法违规收集使用个人信息自评估指南》（“**2019 版自评指南**”）的形式。但是，在内容上结合近年执法中的新情况、新问题，作出了修改。其中，特别值得关注的是：

(1) App 委托的第三方或嵌入的第三方代码/插件存在直接将用户个人信息传输至境外的情况时，应明确向用户告知跨境传输个人信息的目的、类型和接收方等。

(2) App 接入第三方应用时，应提醒用户关注第三方应用收集使用个人信息的规则，**App 运营者不得私自截留第三方应用收集的个人信息。**

(3) 对 App 频繁向用户询问是否同意收集其个人信息的频率划定了标准，即在用户明确表示不同意收集后，**如果 App 在 48 小时内再次询问用户则可能被认定为频繁索权。**

(4) App 存在利用用户个人信息和算法提供定向推送功能的（包括信息和商品展示、广告推送），应向用提供拒绝接受、停止、退出或关闭该功能的机制，或者提供非定制的信息或商品。

(5) 在用户未打开 App 或后台运行 App 时，除业务功能必需的信息外（例如地图 App 导航功能在后台运行时必须收集用户的位置信息），App 不应收集用户个人信息。

(三) 《App 个人信息安全防范指引（征求意见稿）》

信安标委于 2020 年 3 月 30 日发布了《App 个人信息安全防范指引（征求意见稿）》（“**《防范指引》**”），基于信安标委相关统计数据和近期疫情防控类 App 出现的问题，对 App 个人信息安全保护的常见问题进行了梳理并提供了防范策略。其中，特别值得关注的是：

(1) **《防范指引》将小程序明确纳入 App 的监管范畴**，规定 App 是指安装、运行在移动智能终端上的应用软件，包括在应用市场上架的软件、移动智能终端预装的软件、小程序等。

在《防范指引》发布前，主管机关在执法过程中已开始要求对小程序违法违规收集个人信息的行为进行整改。例如，中共天津市委网络安全和信息化委员会办公室于 2020 年 3 月 16 日发布的对疫情防控 App 专项治理情况通报中，即指出了 4 款疫情防控小程序违法违规收集个人信息的情况，并提出整改要求。

从目前监管的态度和执法活动的开展来看，对网络运营者而言，无论其是通过一般性移动应用（App），还是通过第三方平台的小程序提供产品或服务，主管机关对该等行为中涉及的用户个人信息收集和处理行为的合规要求越来越严格，并且主管机关该等要求具体适用在哪些类型的终端表现形式上，这些终端表现形式的范围也会随着市场上产品和服务的形式而不断更新。

例如，曾有相当一段时间，市场对于 App 形式以外的体现形式（例如各类主体提供的小程序）是否需要遵守 App 收集使用个人信息的规范，产生过广泛的讨论。当前，主管部门的执法实践以及《防范指引》明确将小程序这一形式纳入监管范围，有利于广泛的服务提供者明晰自身的合规边界。市场上目前小程序运营者应当对本次《防范指引》的规定予以重视，并应参照《防范指引》对其产品和服务进行自查并及时对违规行为进行修正。此外，小程序运营者在产品开发过程中也应强化个人信息保护的设计。

(2) **针对具有特定用途的疫情防控类 App**，《防范指引》也指出了需要予以关注的问题并提出了具体解决策略，具体如下：

(i) 疫情防控类 App 宜尽可能缩小身份登记的个人信息填写范围，达到可追溯的目的即可。例如，收集个人信息可参考“前台匿名，后台实名”等方式，用户可提供手机号，无需填写身份证号或上传身份证图片。

(ii) 通过个人信息的大数据分析等自动化决策机制来判断用户个人健康状态的，应提供反馈渠道，及时处理因自动化决策机制而严重影响用户个人权益的问题。

二、 个人信息综合性监管规则

(一) 《信息安全技术 个人信息告知同意指南（征求意见稿）》

信安标委于 2020 年 1 月 20 日发布了《信息安全技术 个人信息告知同意指南（征求意见稿）》（“**《告知同意指南》**”）。《告知同意指南》从告知和取得用户同意的适用情形、基本原则、内容方式和具体场景下的特殊规定等方面对网络运营者对个人信息主体进行告知以及收集同意的行为加以规范。其中，特别值得关注的是：

(1) 仅需履行告知义务但不需要获得用户明示同意的情形

《告知同意指南》从个人信息的收集使用、使用目的变更、对外提供等数据处理环节对不需要获得明示同意情形作出了具体规定。相较于最新的《信息安全技术 个人信息安全规范（征求意见稿）》（2019 年 10 月 22 日版）（“**《个人信息安全规范》**”）中的规定，主要变化如下：

(i) 应当进行告知、但无需获得明示同意

《告知同意指南》规定在特定的情形下，免除个人信息控制者取得用户“明示同意”的义务，但不免除“告知义务”。而《个人信息安全规范》则规定在特定的情形下，个人信息控制者无需征得用户的“授权同意”，未对是否需要对用户进行告知作出明确要求。

《告知同意指南》对该等情形的规定，为网络运营者进行个人信息的告知同意提供了更清晰的指导，特别是明确了不免除告知义务，使得网络运营者在起草用户协议和隐私政策的过程中继续注意对这些情形下的个人信息收集和使用进行充分告知。

(ii) 新增免除收集使用个人信息时告知同意的情形

《告知同意指南》增加了收集使用个人信息时仅需要进行告知，不需要取得用户明示同意的情形，主要包括：(i)与商业或职务行为直接相关的个人信息，例如企业依法注册登记、备案的法定代表人、股东、监事、高管等的个人信息；(ii) 用于维护所提供的产品或服务安全和稳定所必需的个人信息，例如软件收集用户的设备类型、网络运行日志、崩溃报告等；(iii) 个人信息控制者为新闻单位且其在开展合法的新闻报道所必需的信息；(iv) 用人单位收集的与个人信息主体求职、就业直接相关的简历等个人信息。

(iii) 使用个人信息目的变更时不强制要求取得用户明示同意的情形

《告知同意指南》增加了在使用个人信息的目的变更时不强制要求取得用户明示同意的情形，即在不会对个人权益带来额外影响的前提下，个人信息控制者可以决定是否采取明示同意方式，主要情形包括：(i) 新目的与原目的具有直接或合理的关联性；(ii) 服务升级、改造导致对用户个人信息的使用频率、展现方式及互动方式调整；(iii) 将个人信息用于学术研究且已进行去标识化处理；(iv) 对使用目的变更进行了安全评估后不存在高风险，且对评估结果进行披露。

(2) 未成年人个人信息的告知同意

(i) 显著加强未成年人网络与信息安全保护是监管趋势的一个重要方面

2019 年我国在未成年人网络与信息安全保护方面显著加强了监管力度。

在监管规则方面，主管部门出台了一系列专门针对未成年人网络与信息安全保护的监管规则。例如，国家互联网信息办公室（“**网信办**”）于 2019 年 8 月 22 日发布《儿童个人信息网络保护规定》；全国人民代表大会常务委员会于 2019 年 11 月 1 日发布了《未成年人保护法》，草案中设置了“网络保护”的专门章节。

在实际监管工作方面，主管部门采取了一系列针对未成年人网络与信息安全保护的专项监管行动。例如，网信办于 2019 年 5 月 28 日统筹 14 家短视频平台和 4 家网络视频平台统一上线“青少年防沉迷系统”；国家新闻出版署于 2019 年 11 月 5 日下发了《关于防止未成年人沉迷网络游戏的通知》严格限制为未成年人提供网络游戏服务时间。

(ii) 进一步细化了对未成年人的监护人进行告知、收集同意的要求

本次公开发布的《告知同意指南》相较于信安标委于 2019 年 10 月 25 日在信安标委成员单位内部发布并征求意见的《信息安全技术 个人信息告知同意指南》草案（“**2019 年《告知同意指南》草案**”），增加了对未成年人的监护人身份的核验要求和核验方式，同时明确了取得监护人同意的具体方式。

(3) SDK (Software Development Kit) 收集使用个人信息场景下的告知同意

《告知同意指南》相比于 2019 年《告知同意指南》草案，进一步明确和强调了接入 SDK 的宿主 App 的主体责任，具体而言：(i) 当 SDK 提

供者不是个人信息控制者时（即提供的 SDK 为功能性 SDK，所采集的个人信息全部为宿主 APP 控制），宿主 App 应告知通过 SDK 收集个人信息的情形并应征得个人信息主体同意；(ii) 当 SDK 提供者仅从宿主 App 间接获取个人信息时，宿主 App 就信息的共享应向个人信息主体进行告知并取得同意；(iii) 当 SDK 提供者是直接个人信息控制者时，SDK 提供者应向个人信息主体告知并应征得个人信息主体同意；(iv) 当 SDK 提供者与宿主 App 同是个人信息控制者时，宿主 App 和 SDK 提供者各自或共同告知个人信息主体并应征得同意。

(4) IoT（Internet of Things）场景下的告知同意

随着智能设备的广泛应用，智能设备中个人隐私泄露事件也时有发生，其中，与智能音箱相关的个人隐私泄露和网络安全事件受到了广泛的关注。

例如，根据新闻报道[1]，美国某知名互联网公司在世界各地雇佣了数千名员工，对旗下智能音箱产品收集的用户语音资料进行标注，但是该公司在其营销和隐私政策材料中没有明确表示其雇佣员工收听该等语音资料。

另外，在国家互联网应急中心网络安全应急技术国家工程实验室联合相关行业企业发布的《智能音箱隐私与网络安全分析报告》中提及，在对市场上部分智能音箱开展了 7*24 小时的流量监控与分析中发现，部分被测智能音箱的上行和下行的绝大部分流量，均为明文数据，未采取严格的安全传输措施，攻击者可以通过伪 AP 等手段，轻易地获取智能音箱采集和传输的各类数据，从而造成用户的敏感数据泄露。此外，中国信息通信研究院中国泰尔实验室发布的《互联网设备-智能音箱安全白皮书（2019 年）》也提及，智能音箱在用户不知情的情况下，过度收集和使用个人信息。智能音箱易出现在用户不知情情况下，对用户语音、位置等敏感信息持续收集的现象，尤其是用户语音，用户较多不易感知；一些智能音箱并未通过隐私政策或其他途径明确告知用户收集使用信息的目的、方式、范围和频次，也未向用户提供明确的允许和拒绝的选择，

这种累积性的权益侵害在日常生活中普遍存在，将会引发用户的严重担忧。信息过度收集使用的乱象亟待解决。

因此，《告知同意指南》针对智能音箱收集和使用个人信息的应用场景，从告知同意的呈现方式、智能音箱对外传输或从其他设备获取个人信息的告知同意情形等方面作出了明确规范。

(5) 车载场景下的告知同意

近年来智能网联汽车相关服务（“**车联网**”）蓬勃发展，在该等业务场景下网络安全与隐私保护也备受关注。

2019 年 10 月 24 日，中国信息通信研究院（“**中国信通院**“）、中国汽车技术研究中心有限公司牵头，联合信安标委相关工作组等各单位，启动车联网（智能网联汽车）网络安全调研及检测评估工作，对我国车联网网络安全现状进行全面摸底，评估掌握车联网安全面临的突出风险及问题，推动健全车联网（智能网联汽车）网络安全管理体系[2]。

2019 年 12 月 25 日，中国信通院在京组织召开专题研讨会，就车联网网络安全防护指南（草案）、车联网数据分类分级及合规应用指南（草案）征求专家意见[3]。

针对车联网这一新的数据合规热点监管场景，《告知同意指南》针对车联设备收集和使用个人信息的情形，从告知同意的呈现方式、同意模式等方面结合车载场景的特殊性作出了明确规范。

(二) 《信息安全技术 - 个人信息安全规范》

2020 年 3 月 6 月，国家市场监督管理总局、国家标准化管理委员会发布了《信息安全技术 - 个人信息安全规范》（“**2020 年信息安全规范**”），并于 2020 年 10 月 1 日起生效。

2020 年信息安全规范生效后将替代 2018 年生效的《信息安全技术 - 个人信息安全规范》（“**2018 年信息安全规范**”），其主要变化如下：增加了“多项业务功能的自主选择”、“用户画像的使用限制”、“个性化展示的使用”、“基于不同业务目所收集个人信息的汇聚融合”、“第三方接入管理”、 “个人信息安全工程”、“个人信息处理活动记录”等内容板块，并对“征得授权同意的例外”、“个人信息主体注销账户”、“明确责任部门与人员”、“实现个人信息主体自主意愿的方法”等内容板块进行了修改。

在 2020 年信息安全规范发布前，信安标委对 2018 年信息安全规范进行了多次修改并更新了多版征求意见稿(最新版本为 2019 年 10 月 24 日左右发布 ,以下简称“**2019 年意见稿**”）,该等修改中的大部分内容已在本次 2020 年信息安全规范中被采纳，同时也在近年主管部门网络安全与数据合规的排查和整顿工作中得到贯彻落实，已经反映在 2020 年信息安全规范颁布前的一系列重要整顿文件中，以及反映在许多 APP 的隐私政策文本和 APP 的实际设计当中。

举例而言，该等修改中要求，不得强迫个人信息主体一次性接受并授权多项业务功能的个人信息收集，在此前国家互联网信息办公室等主管机关发布的《App 违法违规收集使用个人信息行为认定方法》及 App 专项治理工作组推进的专项整治行为中都得到了体现和落实。

本文就 2020 年信息安全规范中体现的对 2018 年信息安全规范及 2019 年意见稿的主要修改进行了梳理和分析，其中特别值得关注的有：

(1) 删除了个人信息控制者“不应大规模收集中国公民“种族、民族、政治观点、宗教信仰等个人敏感信息”的表述

该等删减可能考虑到在实践中存在的一些网络运营者受国家机关委托进行此类信息收集和处理工作的情况，为避免对企业和其它单位的业务和工作开展设置不必要的障碍，进行了这项调整。

同时，2020 年信息安全规范也关注到“种族、民族、政治观点、宗教信仰”等个人敏感信息的重要性，一旦泄露，可能会对国家和社会安全与稳定造成威胁，因此要求个人信息控制者不应披露对前述信息的分析结果。

(2) 对收集、存储、共享和转让个人生物识别信息的特殊要求

(i) 收集个人生物识别信息应当单独告知个人信息主体相关规则并获得其授权

个人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。

考虑到个人生物识别信息对个人人身和财产安全的重要性及全球范围内的个人生物识别信息泄露的担忧，2020 年信息安全规范对收集个人生物识别信息的授权提出更为严格的要求，要求个人信息控制者“单独告知”并取得个人信息主体的“明示同意”。

从操作上看，对收集个人生物识别信息的行为制定单独的隐私政策可能是满足这一要求的更好的实践；同时，就该等声明或规则还应以弹窗等方式向个人信息主体发布并实现个人信息主体以主动勾选等明示同意方式作出授权。

(ii) 个人生物识别信息的存储要求

(a) 个人生物识别信息应与个人身份信息分开存储。就此，个人信息控制者应当考虑对分类收集和存储个人信息，并在内部系统中采用数据隔离墙等技术措施实现该等要求。

(b) 个人信息控制者原则上不得存储原始个人生物识别信息，可采取的措施包括：

- 存储无法回溯到原始生物识别信息的摘要信息；

- 在采集终端中使用个人生物识别信息完成身份认证等功能，即个人生物识别信息仅存储在个人信息主体的采集终端（如手机）上，个人信息控制者仅取得采集终端回传的个人生物识别信息验证结果，作为操作的依据，避免对个人生物识别信息直接存储；

- 在个人信息控制者完成身份认证等工作后，立即删除可提取个人生物识别信息的原始图像。即当因个人信息控制者的技术、系统或设备等各种原因无法在采集终端完成对个人生物识别信息识别或处理时，在个人信息控制者完成对该等信息的处理后，应立即删除其系统中留存的可提取个人生物识别信息的原始图像。

(iii) 共享和转让个人生物识别信息的特殊要求

个人生物识别信息原则上不应共享、转让。因业务需要，确需共享、转让的，应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意

(3) 对个人信息主体注销账户要求的修改

(i) 不再要求个人信息控制者必须设置“注销功能交互式页面”；

(ii) 明确个人信息控制者对注销账户请求的响应时限不得超过 15 个工作日，该等要求与《App 违法违规收集使用个人信息行为认定方法》中关于注销账户的承诺时限基本保持一致[4]；

(iii) 对于存在必要业务关联关系的产品和服务的部分注销，应当主动提示个人信息主体注销的详细后果，包括一旦注销某个产品或服务的

账户，将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等后果的说明；

(iv) 在多个产品和服务共用同一账户的情况下，注销账户时可能对没有独立的账户体系的产品或服务产生影响时，可采取对账号内该等产品或服务以外的其他个人信息删除的方式，并切断账户体系与该等产品或服务的关联，从而实现保留产品和服务与待注销账户的分离；

(v) 个人信息主体注销账户后，应及时删除其个人信息或做匿名化处理。因法律规规定需要留存个人信息的，不能再次将其用于日常业务活动中。

(4) 采用交互式页面提供产品或服务的个人信息控制者，宜设置便捷的交互式页面以响应个人信息主体的请求

2020 年信息安全规范对采用如网站、移动互联网应用程序、客户端软件等交互式页面方式提供产品或服务的企业，响应个人信息主体的访问、更正、删除、撤回授权同意、注销账户等各类请求提出了更高的合规要求；但是，在目前的实践中，该等企业仍存在以交互式页面提供产品或服务的企业通过邮件、电话等方式响应个人信息主体请求的情况有待改善。

(5) 任命专职个人信息保护负责人和个人信息保护工作机构的门槛调整

2020 年信息安全规范对需要设置专岗专人进行安全保护的要求进行的调整 ,其中 :(i) 修改了处理个人信息数量的门槛从 50 万增加至 100 万；(ii) 对处理个人敏感信息需要设立专职的个人信息保护负责人和个人信息保护工作机构的情形，增加了处理超过 10 万人的个人敏感信息的门槛。

(三) 《中华人民共和国民法典》

全国人民代表大会于 2020 年 5 月 28 日通过了《中华人民共和国民法典》（“**《民法典》**”），该法典将于 2021 年 1 月 1 日起正式施行。《民法典》“人格权编”第六章延续了《中华人民共和国民法总则》和《网络安全法》中对个人信息的相关保护规定，并且进一步明确了处理个人信息的原则和条件、自然人的个人信息救济权利、信息处理者个人信息保护义务、法定机构及其工作人员对个人信息的保密义务等内容。其中，特别值得关注的是：

(1) 《民法典》对个人信息与隐私权作出了衔接：根据《民法典》第 1034 条规定，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。由此可见，当自然人被侵害的信息既属于个人信息又属于私密信息时，其可以选择适用隐私权保护的规定保护其利益，当隐私权无法保护其权益时，也可适用于关于个人信息保护的规定。

(2) 个人信息权益的救济方式：除可以要求侵权主体承担侵权责任外，《民法典》参考《信息安全技术 个人信息安全规范》的相关要求，规定当自然人的个人信息遭受或可能遭受特定情况的损害时，其还可以向信息处理者查阅或者复制其个人信息；发现信息有错误的，有权提出异议并要求更正；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，自然人有权要求删除其个人信息。

(3) 信息处理者处理个人信息的免责事由：《民法典》规定，信息处理者处理个人信息的行为在特定条件下可以不承担民事责任，具体条件包括：该行为是在自然人或者其监护人同意的范围内合理实施的；该行为是在合理处理该自然人自行公开的或者其他已经合法公开的信息（但是，该自然人明确拒绝或者处理该信息侵害其重大利益的除外）；该行为是为维护公共利益或者该自然人合法权益，合理实施的其他行为。

(四) 《浙江省公共数据开放与安全管理暂行办法》

浙江省人民政府于 2020 年 6 月 12 日发布了《浙江省公共数据开放与安全管理暂行办法》（“**《暂行办法》**”），该办法将于 2020 年 8 月 1 日起正

式施行，对浙江省行政区域内的公共数据开放、利用和管理作出了规定。其中，特别值得关注的是：

(1) 公共数据的范围和分类：指各级行政机关以及具有公共管理和服务职能的事业单位，在依法履行职责过程中获得的各类数据资源。根据数据开放的风险程度，将公共数据分为无条件开放、受限开放、禁止开放三类，并针对不同风险类别设置了有差异的开放方式。

(2) 禁止开放的公共数据

(i) 依法确定为国家秘密的；
(ii) 开放后可能危及国家安全、公共安全、经济安全和社会稳定的；
(iii) 涉及商业秘密、个人隐私的；
(iv) 因数据获取协议或者知识产权保护等禁止开放的；
(v) 法律、法规规定不得开放或者应当通过其他途径获取的。

前述(i)-(v)款所列的公共数据，依法已经脱敏、脱密等技术处理，符合开放条件的，可以列为无条件开放类或者受限开放类公共数据。

前述(iii)款所列涉及商业秘密、个人隐私的公共数据不开放将会对公共利益造成重大影响的，公共数据开放主体可以将其列为无条件开放类或者受限开放类公共数据。

(3) 受限开放的公共数据

(i) 涉及商业秘密、个人信息的公共数据，其指向的特定公民、法人和其他组织同意开放，且法律、法规未禁止的；
(ii) 开放将严重挤占公共数据基础设施资源，影响公共数据处理运行效率的；
(iii) 开放后预计带来特别显著的经济社会效益，但现阶段安全风险难以评估的。

公民、法人和其他组织可以向公共数据开放主体提出获取受限开放类数据的服务需求，但应当符合规定的数据存储、数据处理、数据安全保护能力等条件并达到相应的信用等级。

后记：

海问在网络安全、数据合规领域积累丰富的经验，亦持续关注不断更新的法律法规及与数据合规有关的时事热点。您可通过如下链接浏览此前的《海问观察：网络安全及数据合规动态》：

《海问观察：网络安全及数据合规动态》（2019 年 9 月上半月）
《海问观察：网络安全及数据合规动态》（2019 年 9 月下半月-10 月上半月）
《海问观察：网络安全及数据合规动态》（2019 年 10 月下半月-11 月）
《海问观察：网络安全及数据合规动态》（2019 年 12 月）

---

[1] 来源请见凤凰科技报道，网址：https://tech.ifeng.com/a/20190411/45589702_0.shtml。

[2] 来源请见工业和信息化部报道，网址：http://www.miit.gov.cn/n1146290/n1146402/n1146440/c7490194/content.html。

[3] 来源请见中国信通院报道，网址：https://mp.weixin.qq.com/s/bmqCErOv-OFJu07Kjq4kyQ。

[4] 根据《App 违法违规收集使用个人信息行为认定方法》第六点第 3 条，虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。