从《个人信息保护法》角度解读中国企业隐私合规

敏于知

企业数字化转型趋势以及隐私保护

2021 年对于企业数字化转型工作来说，是充满了机遇和挑战的一年。随着国家不断出台如《数字化转型伙伴行动倡议》、《中小企业数字化赋能专项行动方案》等推动企业数字化转型的系列政策，宏观环境对于企业数字化转型工作的扶持、鼓励力度正不断加大。

现代企业在日常经营中将无可避免地采集、储存并处理用户产生的各类数据。随着近年来各行业互联网业务的不断普及，客户在其中积累了大量数据。综合使用这些数据、建立用户画像，并针对性地通过不同形式向不同客户投放不同广告，成为了头部企业最为普遍的获客方式。但由于此类方式需大量收集并分析客户数据，客户感知到的针对感及侵入感较强，因此，客户数据收集及处理相关的合规成本及潜在监管罚款可能显著地推高了企业的总体营销成本。

隐私保护帮助企业解决数据使用中的挑战

由于客户数据的潜在敏感性，不当收集及处理相关数据可能侵害数据主体的权益，导致企业遭遇监管机构的处罚，产生财务及声誉损失。因此，如何兼顾数据应用效率和合规性，成为了近期企业数字化转型工作的重要议题。如何合规使用，合理保护客户数据以减少客户的负面观感，成为了现代数字化企业的一大挑战。有效的数据隐私保护可获取客户的信赖，最终增加品牌声誉，加大用户粘性。甫瀚认为，有效的隐私保护是解决相关挑战的重要抓手。

《个人信息保护法》法律框架与主要条文解读

模块	覆盖条文	主要条文解读
适用范围	第 1-12 条	▪ 域外效力（第 3 条）：“在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法。（一）以向境内自然人提供产品或者服务为目的；（二）分析、评估境内自然人的行为；（三）法律、行政法规规定的其他情形。”此规定与 GDPR 的“长臂管辖”原则有一定类似，规定了法案的域外效力。 ▪ 个人信息处理的生命周期（第 4 条）：“个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除。”
个人信息处理原则与认定标准	第 13-37 条	▪ 敏感个人信息（第 28 条）：“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，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。”将个人信息与个人敏感信息加以区分。 ▪ 自动化决策情形下的处理规则（第 24 条）：“通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。”回应了“大数据杀熟”的问题，进一步规范了企业在使用互联网进行商业活动的隐私安全责任。 ▪ 单独同意（第 23、25、26、29、39 条）：《个人信息保护法》首先提出了“单独同意”的概念，规定了不同的需要单独同意的情景。

数据跨境传输规则	第 38-43 条	▪ 分类分级制的个人信息跨境传输规则（第 38、40 条）：“按照国家网信部门的规定经专业机构进行个人信息保护认证；”“关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。”此规定给个人信息跨境传输提供了指导。
个人信息主体的权利	第 44-50 条	▪ 知情权、决定权（第 44 条）。 ▪ 可携带权（第 45 条）。 ▪ 自然人死亡其近亲属权利（第 49 条）：“自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利。”
个人信息处理者的义务	第 51-59 条	▪ 采取安全保障措施的义务（第 51 条）。 ▪ 进行合规审计的义务（第 54 条）。 ▪ 影响评估义务（第 55、56 条）。 ▪ 个人信息泄露、篡改、丢失事件的通知、采取补救措施的义务（第 57 条）。 ▪ 特殊义务（第 58 条）：规定了提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行的义务。
个人信息保护职责部门	第 60-65 条	▪ 各部门职责（第 60-65 条）：规定了国家网信部门、国务院有关部门和县级以上地方人民政府有关部门的职责。
法律责任	第 66-71 条	▪ 行政处罚（第 66 条）：责令改正、给予警告、没收违法所得、责令暂停或者终止服务，也包括罚款。根据情节严重程度不同对个人处以 1 万至 100 万不等的罚款，对企业处以 5000 万以下或上一年营业额 5% 以下的罚款。 ▪ 公益诉讼（第 70 条）：人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。 ▪ 刑事处罚（第 71 条）：违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

中外隐私保护法律存在差异

中外在隐私安全规范的进程各有异同，我们通过下表从多个维度进行比较，呈现了中国《个人信息保护法》、欧盟 GDPR 和美国加州 CCPA&CPRA 的异同。[1]

对比维度	个保法	GDPR	CCPA&CPRA
地域范围的宽泛度	中	高	低
合法性基础与同意规则的严格度	高	中	低
个人信息定义与敏感信息处理规则的严格度	高	高	低
受规制对象类型的严格度	中	高	低

从上表可看出，中国《个人信息保护法》在规则的严厉程度上基本对标欧盟 GDPR，加州隐私立法（CCPA&CPRA）相较于其他两部法律更为宽松。

[1] 腾讯研究院《中美欧个人信息保护法比较——以中国个人信息保护法、欧盟 GDPR，美国加州 CCPA&CPRA 为样本》：https://www.tisi.org/19493。

《个人信息保护法》背景下重点行业主要隐私风险

2015 年，国务院印发《关于积极推进“互联网 +”行动的指导意见》，传统的产业加速实现“互联网 +”改革，各行各业已与互联网融合为社会提供新的运作模式，在这个过程中，数据隐私风险也越来越值得关注。根据 OWASP 的调研[2]，2021 年的十大隐私风险分别是：Web 应用程序漏洞、运营商端的数据泄露、数据泄露事件响应不足、滥用同意、不透明的政策和条款、个人数据删除不足、数据质量不足、会话超时缺失或不足、用户无法访问和修改数据，以及收集除用户同意范围之外的数据。

《个人信息保护法》出台后，重点行业需要关注以下隐私风险：

一、汽车行业需要关注车联网的隐私安全问题

车联网具有计算、存储和通信功能，可以与其他车辆沟通合作，提高用户的驾驶安全和驾车体验，为自动驾驶技术的进一步发展提供可能性，是智慧城市的重要组成部分。车联网带来的典型隐私问题包括 “一是超范围采集用户信息，肆意跨越数据采集边界。二是车联网数据跨境传输可能脱离我国互联网防火墙限制，造成地理位置等国家重要数据泄露。三是数据非本地化存储带来潜在的国家安全隐患。”[3]

二、医疗行业需要关注个人医疗数据、医疗实验数据、科研数据等的隐私和安全

医疗数据的来源和范围具有多样化的特征，如临床药物实验信息、基因遗传、医学实验、科研数据等。个人的医疗数据关系到个人的隐私保护，而医疗实验数据、科研数据不仅关系到数据主体的隐私、行业发展，甚至关系到国家安全。在数字化趋势下，药品追踪、体征监测、移动护理等信息平台和物联网应用场景的广泛使用，为管理和运营增加了一定的数据安全风险。同时，制药行业具有更复杂的隐私监管合规要求，COVID-19 疫情加速了医药行业的信息化和数字化，给行业带来了更多的管理、创新研发和医疗资源配置中的隐私保护挑战。

三、零售行业需要特别关注电商的隐私保护问题

电子商务涉及的具体商品与服务种类丰富，收集使用的个人信息类型繁杂。以提供通用商品与服务交易的“淘宝”为例，其会收集用户的会员信息、设备信息、服务日志信息、订单信息、支付信息、物流信息等。电子商务服务收集的用户个人信息敏感程度普遍较高。电子商务因为涉及交易和物流等必要环节，均可能需要收集“用户账户资金、交易订单、身份证件信息、家庭住址”等个人敏感信息。[4]

四、金融行业需要关注网络支付、借贷等互联网金融的隐私保护问题

人工智能和生物识别技术在金融行业广泛使用，如基于图像识别技术的人脸、表单、票据等识别系统（人脸支付、证券账户远程开户等）与指纹识别、人脸识别、虹膜识别等，使得金融行业收集大量的个人敏感数据。互联网金融中消费者隐私被侵害主要以金融机构擅自收集、擅自泄露消费者隐私信息、跟踪消费者网站浏览记录为主要形式。[5] 互联网金融需要强监管，才能保障消费者的个人隐私不被侵犯。

[2] OWASP Top 10 Privacy Risks：https://owasp.org/www-project-top-10-privacy-risks/。

[3] 车联网的数据安全问题 [J]，王伟洁，网络安全和信息化，2021(06):45：https://kns.cnki.net/kcms/detail/detail.aspx?FileName=WAXX202106018&DbName=CJFQ2021。

[4] “互联网 + 行业”个人信息保护研究报告（2020 年）：http://www.caict.ac.cn/kxyj/qwfb/bps/202003/P020200302576687898634.pdf。

[5] 互联网金融消费者隐私保护探析 [J]，杜宏，内蒙古财经大学学报，2021,19(01):108-111：https://kns.cnki.net/kcms/detail/detail.aspx?FileName=NMCJ202101028&DbName=CJFQ2021。

企业的应对之道

随着《个人信息保护法》的出台，企业必须在该背景下做出积极应对。从短期来看，企业可以对企业现存个人信息进行识别、梳理、分类分级管理，加强人员关于个人隐私的安全教育培训，在涉及数据跨境的传输之前做好评估与申报。

从长期来看，企业应该做好以下几点来积极响应国家对个人隐私的保护：

- 采取安全技术措施保障个人隐私数据的保护
- 设置数据保护办公室或其他角色负责数据管理与保护
- 制定内部隐私管理制度、流程和操作规则
- 定期进行隐私保护合规审计
- 制定隐私安全事件应急预案，定期举行应急演练

只有将隐私保护纳入公司章程，将隐私保护的概念深入人心，运用专业的技术和管理来进行隐私保护，企业才能对公众、社会与国家尽到相应的责任，维护社会稳定，协助经济发展。此外，对比本土企业，跨国企业需要在隐私安全保护方面付出更多的资源。

对比维度	跨国企业	本土企业
数据本地化成本	为建立中国境内的数据中心，实现本地化存储，跨国公司需付出较大成本用于基础建设的改造、人力资源的增补等。	数据中心大多数在中国境内，数据跨境传输的需求较少，合规成本相对低。
数据跨境规则复杂度	跨国公司要符合不同国家的数据跨境传输的监管要求，面临着不同国家的业务节点部署的合规要求。	数据跨境传输需求较少，规则较为单一。
合规要求与业务要求的冲突	某些不允许跨境传输的数据，可能是业务运营的关键，解决合规要求和业务要求冲突的成本可能较高。	业务所要求的数据鲜有面临因不符合跨境传输要求而无法获得的问题。

达于行

甫瀚可提供的服务

甫瀚为企业提供隐私保护管治咨询，从治理、合规及技术角度，全面协助企业提升隐私保护水平，达成隐私保护从无到有、从弱到强的转变，为优化企业综合信息安全治理水平奠定基础。我们可提供的隐私相关服务包括：数据隐私法规合规性评估、数据安全咨询、隐私托管服务、隐私工具实施服务、事件响应取证，及安全意识与能力咨询服务。

甫瀚基于隐私保护实践，制定隐私保护提升方法论。通过解读法律法规要求、理解企业内外部环境等方式，锚定企业隐私保护基线，确定能力差距；通过技术选型、控制策略制定等方式，搭建企业隐私保护方案，确保符合法规要求及企业经营需求；通过持续合规评估、控制策略维护等手段，确保企业隐私保护方案拥有长期效力，使隐私保护真正成为企业的核心竞争力。

关于甫瀚咨询

甫瀚咨询是一家全球性的咨询机构，为企业带来领先的专业知识、客观的见解、量身定制的方案和卓越的合作体验，协助企业领导者们充满信心地面对未来。透过甫瀚咨询网络和遍布全球20多个国家的逾85家分支机构和成员公司，我们为客户提供财务、信息技术、运营、数据、分析、治理、风险管理以及内部审计领域的咨询解决方案。

甫瀚咨询荣膺2021年《财富》杂志年度最佳雇主百强，我们为超过60%的财富1000强及超过35%的全球500强企业提供咨询服务，亦与政府机构和成长型中小企业开展合作，其中包括计划上市的企业。甫瀚咨询是Robert Half International Inc.（纽约证券交易所代码：RHI）的全资子公司。RHI于1948年成立，为标准普尔500指数的成员公司。

联络方式

北京

朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话：(86.10) 8515 1233

上海

徐汇区陕西南路 288 号
环贸广场二期 1915-16 室
电话：(86.21) 5153 6900

深圳

福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话：(86.755) 2598 2086

香港

中环 干诺道中 41 号
盈置大厦 9 楼
电话：(852) 2238 0499

protiviti® 甫瀚