2021. 11. 1

中国风险消息<2021.No.4>

个人信息保护法解析

本文由上海开泽律师事务所合伙人律师王稳撰稿。

【要点】

- 2021 年 8 月 20 日，在十三届全国人大常委会第三十次会议上，表决通过了《中华人民共和国个人信息保护法》，自 2021 年 11 月 1 日起正式施行。
- 与个人信息保护相关的规定大多分散在不同的规范性文件中，但随着《中华人民共和国个人信息保护法》的制定，完善了个人信息保护应遵循的原则和个人信息处理规则，明确了个人信息处理活动中的权利义务边界。
- 在本文中，我们将阐述《中华人民共和国个人信息保护法》的概要，并结合案例对应把握的要点进行解读。

一、概述

随着互联网时代的发展，保护个人信息安全、规范个人信息处理活动也显得尤为重要，在《中华人民共和国个人信息保护法》（以下简称“《个人信息保护法》”或“该法”）出台之前，与保护个人信息相关的规定大多分散于不同的规范性文件中，如《关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》《信息安全技术个人信息安全规范》等。

尽管中国政府启动《个人信息保护法》的立法研究时间较早，且其他与此相关的规范性文件对个人信息的保护也起到了一定的约束性作用，但近年来，一些涉及侵犯个人信息的典型案例引起社会的持续强烈反响，在一定程度上也加快了《个人信息保护法》的立法进程。

<个人信息使用不当的案例>

时期	事件
2019 年	工业和信息化部组织对 61 家互联网企业和 51 家手机应用商店的应用软件进行检查发现，许多网站和应用中存在未经用户同意收集使用用户个人信息的情况。
2020 年	全国公安机关网安部门充分发挥职能作用，加大公民个人信息保护力度，依法查处违法违规收集公民个人信息 APP 服务单位 386 个，涉及信息咨询、辅助学习、文学小说、新闻资讯、娱乐播报等多个类型。
2021 年 7 月 4 日	国家网信办发布通报称，“滴滴出行”APP 存在严重违法违规手机使用个人信息，已通知应用商店下架并要求整改。而早在 2020 年 11 月，“滴滴出行”就宣布国内月活用户突破 4 亿。

基于社会对个人信息保护立法的呼声越来越强烈，2021 年 8 月 20 日，第十三届全国人民代表大会常务委员会第三十次会议通过《个人信息保护法》，并将于 2021 年 11 月 1 日正式施行。

全文共八章七十四条，该法明确了个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作机制。

确立以“告知—同意”为核心的个人信息处理规则，落实国家机关保护责任，加大对违法行为的惩处力度。其中，该法涉及的个人信息保护的主要原则包括：

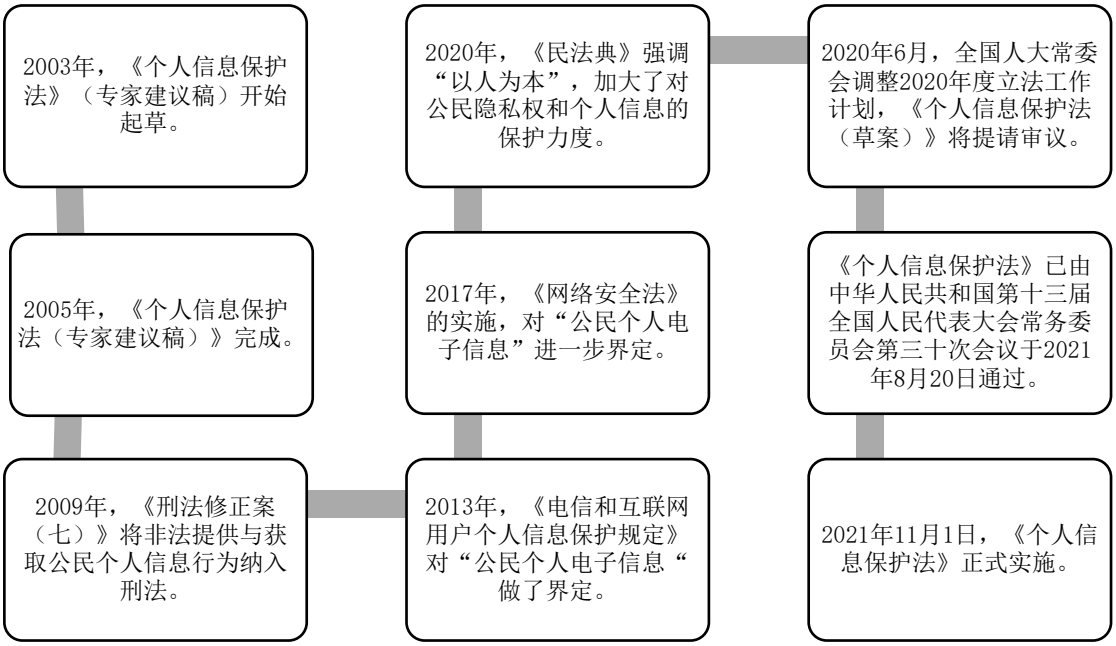
〈个人信息保护的主要原则〉

原则	内容
合法正当诚信原则	处理个人信息应当遵循合法、正当、必要和诚信原则，不得误导、欺诈、胁迫等方式处理个人信息。
目的明确原则	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，采取对个人权益影响最小的方式。
最小必要原则	收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。
公开透明原则	处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明确处理的目的、方式和范围。
信息准确原则	处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。
安全保障原则	个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

二、修订沿革

2003 年启动《个人信息保护法》的立法研究至 2021 年 11 月 1 日即将正式实施日止，《个人信息保护法》的立法历程显得尤为艰辛与坎坷。既经历了机构改革、立法资源制约的困顿，也因个别案件而加速该法的立法进程。其中，2016 年 8 月 21 日，徐玉玉作为大学生，被诈骗电话骗走上大学的学费 9900 元，伤心欲绝导致心脏骤停，经抢救无效不幸离世，后该案被最高检和公安部联合挂牌督办。“徐玉玉案”因此也获得最高院评选的“2017 年推动法治进程十大案件”。

此外，《个人信息保护法》草案在经历全国人大常委会审议的过程中，也因学界、企业和立法机构代表各自立场不同，发生了不少条款上的碰撞。如死者的个人信息是否应当得到积极保护；是否需要建立统一的个人信息保护监管机构等等。经过了十几年不断的摸索，个人信息保护立法才逐渐趋于完善。



三、重点解说

结合现有生效法律文件中对个人信息保护的相关规定，《个人信息保护法》在基于中国现行实践及国际经验的基础上，形成了一部相对健全的法律文件。

(一) 明确了“个人信息”与“敏感个人信息”的范围

根据该法第四条之规定，“个人信息”是指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。

作为界定个人信息范围的补充，2017 年 6 月 1 日施行的《网络安全法》第七十六条也规定，个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

需要特别提醒注意的是，该法第二十八条首次通过列举的方式将“敏感个人信息”的范围进行了罗列，具体包括个人的生物识别、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。

【要点】

《个人信息保护法》通过概述和列举的方式对受保护的个人信息范畴进行了明确，公司在进行类似的个人信息保护合规管理中，可以参照适用。当然作为除外规定，该法明确了匿名化信息不属于保护信息，照此来看，公司在使用个人信息中如隐去个人姓名等身份信息后的处理则不属于个人信息的处理范畴，处理风险相对较低。

(二) 强调“个人信息”与“敏感个人信息”的处理规则

根据该法第十三条之规定，区分不同的情形，一般情况下的个人信息处理需取得个人同意。在规定的情形（包括：人力资源管理；履行法定职责或法定义务；应对突发公共卫生事件；紧急情况下保护自然人生命健康和财产安全所必需等等）中，此类个人信息的处理不需要取得个人同意。

当然，在“敏感个人信息”的处理规则中，因敏感个人信息一旦被泄露或非法使用，容易导致自然人的人格尊严或人身、财产等受到侵害，故而，根据该法第二十八条、第二十九条之规定，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。同时，处理敏感个人信息应当取得个人的单独同意。

【要点】

通过上述“个人信息”与“敏感个人信息”的处理规则比较来看，在均需个人单独同意的情形下，敏感个人信息的处理对公司的要求更高，公司不仅需要事先明确处理的特定目的及充分的必要性，而且还需采取严格的保护措施。

(三) 为个人赋予撤回同意的权利

根据该法第十五条之规定，基于个人同意处理个人信息的，个人有权撤回其同意。在具体撤回时，也要求个人信息处理者应提供便捷的撤回同意方式。就“便捷”而言，依照相关国家标准的精神，其便捷程度宜与给予授权的便捷程度相对等。此外，第十五条明确撤回同意不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

【要点】

尽管“敏感个人信息的处理规则”中并未明确为个人赋予撤回同意的权利，但结合上下文综合来看，赋予撤回同意的相关规定系列于个人信息处理规则的一般规定中，而敏感个人信息的处理属于特别规定，在特别规定无明确禁止或除外约定的情形下，该撤回同意的权利应同样适用于敏感个人信息。

(四) 确立的自动化决策的处理原则

随着信息技术的高速发展，作为个人信息的处理者，如通过事先预设的程序对个人信息进行读取、存储等自动化决策时，应保证决策的透明度和结果公平、公正。

结合生物识别、算法、数据使用等技术手段所形成的营销手段，该法第二十四条之规定，通过自动化决策方式向个人进行信息推送、商业营销，应同时提供不针对其个人特征的选项，或者提供便捷的拒绝方式。

特别是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。

【要点】

从立法者的本意来看，立法者也不排斥经营者通过高科技手段从事相关的市场营销活动，但该营销活动不应以侵犯个人信息为前提，同时必要的审慎责任，对可能对个人权益产生影响的推广行为进行必要的约束。

(五) 全面规范个人信息跨境提供的规则

该法第三章专门对个人信息跨境提供的规则进行了全面的规范，就个人信息处理者因业务需要需向境外提供个人信息的，作出了相对严苛的前置性限定条件，应具备包括通过国家网信部门组织的安全评估；经专业机构进行个人信息保护认证；根据国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利义务等在内的任一条件。

当然，从个人信息保护角度来讲，个人信息跨境提供需向个人明确告知境外接收方的相关信息并获得个人的单独同意。在一定程度上，这也增加了个人信息处理者必要的安全保障义务。

【要点】

因个人信息跨境提供可能涉及的国家安全问、公共利益等相关重大利益，个人信息处理者拟跨境提供时应做好充分的事先安全评估或个人信息保护认证等相关工作，以避免不必要的行政监管。

(六) 对违反个人信息保护的行为设置了严苛的法律责任

考虑到在侵害个人信息行为可能带来的严重后果，该法第六十六条、第六十七条及第七十一条对违反该法规定处理个人信息或未履行该法规定的个人信息保护义务的，给予相对严苛的法律责任，具体包括：

处罚类型	处罚内容
行政处罚	① 对违反该法规定处理个人信息，或处理个人信息未履行个人信息保护义务的，给予责令改正，给予警告，没收违法所得；对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 ② 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、级管理人员和个人信息保护负责人。
计入信用档案	有该法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。
治安管理行为	构成违反治安管理行为的，依法给予治安管理处罚。
刑事责任	构成犯罪的，依法追究刑事责任。

同样，考虑到侵害个人信息可能涉及的覆盖面较广，人员较多，该法第七十条也明确约定了公益诉讼的内容，即如侵害众多个人的权益的，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。

【要点】

因违法的法律责任确实较为严苛，个人信息处理者应尽可能避免不必要的行政监察。当然，从公益诉讼的角度来讲，部分行业巨头等头部企业被行政部门列为存在违法行为嫌疑的，很有可能会成为该类诉讼的目标。

(七) 明确个人信息侵权行为的归责原则为过错推定

对于个人信息处理者侵害个人信息权益造成损害的，该法约定了过错推定的归责原则。根据该法第六十九条之规定，如个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。就具体损害赔偿责任而言，损害赔偿的金额首先按个人因此受到的损失或个人信息处理者由此获得的利益确定，无法确定前述金额的，根据实际情况确定赔偿数额。

【要点】

个人信息侵权行为的归责原则参照了《民法典》中侵权责任篇的内容。这也提醒企业在实践中尽可能保留与合规使用个人信息的证明文件、使用痕迹等必要证据。

四、案例概述

案例 A	2011 年至 2013 年 9 月，A 某、B 某在分别担任某世界 500 强外资食品饮料企业的中国公司的西北区婴儿营养部市场经理、兰州分公司婴儿营养部甘肃区域经理期间，为了抢占市场份额，安排公司另外 4 名员工为推销奶粉，通过支付好处费等手段，从兰州多家医院获取孕产妇姓名、手机号等信息共计 12 万余条。2016 年 10 月 31 日，法院一审判决，以侵犯公民个人信息罪分别判处 A 某等人拘役 4 个月至有期徒刑 1 年 6 个月不等的刑罚。之后，相关员工以涉案行为属于单位犯罪等理由提出上诉。2017 年 5 月 31 日，兰州市中级人民法院作出二审终审裁定：驳回上诉，维持原判。
实例 B	2020 年 5 月 6 日，脱口秀演员 C 某发布微博称，在其与经纪公司 D 公司的经纪合约纠纷案中，E 银行未获 C 某本人授权，将其个人账户流水提供给 D 公司，属于侵犯公民个人信息的违法行为。后 E 银行书面公开致歉，就银行担当员工未按规定办理相关业务手续给 C 某导致的麻烦表示郑重道歉。同时，该行对相关员工予以处分，并对支行行长予以撤职处分。

上述两个案例均涉及侵犯个人信息的行为，案例 A 中，外资食品饮料公司的中国员工为抢占市场，违法购买潜在客户群体的个人信息，社会负面影响极其恶劣，也使得该公司的商业信誉显著降低。而案例 B 的 E 银行的事例，则是其业务人员操作不规范导致不当泄露银行用户信息，因此次事件用户身份特殊而得到社会广泛关注，同时也反映出该行针对用户信息的管控制度不健全、存有重大漏洞。

五、企业合规建议

作为在华日企，接触并使用包括员工信息、客户信息在内的个人信息时，应进行有效地风险防范操作以避免发生不必要的纠纷。

整体上来看，随着该法的颁布实施，将对包括在华日企在内的外商投资企业使用个人信息的合规要求程度将越来越高，但是同时个人信息相关事件或者被侵权的事件还是会不断发生，也应切实需要避免因不当使用个人信息导致不必要的风险。根据我们以往的实践，在华企业在有可能会面临如下场景：

1. 员工抵触提供包括敏感个人信息在内的个人信息；
2. 员工在同意公司使用个人信息又主动撤回；
3. 员工对公司使用个人信息的处理目的、处理方式等提出异议的；
4. 员工恶意主张公司存在违反该法并导致损失的情况等。

同时，个人信息泄露事件严重者，甚至会被不法分子利用而进行诈骗等行为，届时，个人信息管理者、处理者将承担相应的法律责任。因此，公司在做好个人信息保护管理的整个流程中，需依据该法要求，在信息保护（泄露）前、中、后三个时期做好相应的对策，以避免后续法律责任的承担。在此过程中，避免不了公司要进行一系列的规章制度的完善与制订、员工的个人信息保护意识培训以及与国家互联网信息办公室等相关行政部门的沟通，及时确认政策法规的更新与变化，尽可能及时应对公司管理中的个人信息保护漏洞。

作为个人信息的管理者、使用者的企业将被要求主动的采取个人信息保护措施，降低个人信息侵权事件的发生，还有更重要的是，万一发生非企业故意发生个人信息侵权事件时，企业建立了完整的个人信息保护制度，平时定期进行个人信息保护的培训和考评，发生事件时即使采取合法合理的应对，可以减轻或者免除企业的责任。具体合规的要求简要包括：

1. 公司作为员工的管理者，系员工个人信息管理的直接责任主体。实际操作中，公司应根据内部组织结构，确定专门的部门（如总务部、人事部等）进行员工个人信息的保管、管理及使用。
2. 作为获得员工授权的最佳时间，新员工办理入职时及要求提交书面同意材料，老员工则在给予福利（体检、旅游等）前安排签署。实践中，可能会出现部分员工拒绝提供个人信息的情况，该情况下，从员工的有效管理角度，建议结合员工的实际顾虑进行针对性的解决，如通过日常合规培训、团队凝聚力建设等来获得此类员工贵司公司工作的理解与支持。
3. 收集及处理个人信息仍需要获得员工的书面同意。同意的内容应尽可能体现员工明确知晓公司使用个人信息的用途、方式等，并在此基础上同意公司使用。
4. 员工的宗教信仰、体检报告、银行账户、行踪轨迹等属于敏感个人信息，应采取特别的保护措施，如电子文档可以设置加密信息；纸质文档必要时应配备专门保管仓储设备。
5. 在处理客户信息时，应尽可能仅限于工作范围内进行公开和使用，这也对员工如何合规使用也提出了更高的要求，建议公司在建立类似合规制度的基础上，定期或不定期组织类似合规要点的培训活动，以增强员工的合规意识。

全文完

撰稿:上海开泽律师事务所 合伙人律师 王稳

〈作者简历〉
◆ 王稳
曾先后就读于日本东京大学法学部、日本一桥大学法学研究科，并于 1999 年开始从事律师执业活动。2004 年在上海成立了上海开泽律师事务所。王稳律师在深入理解中日间商业、法律、文化、思维和倾向的差异与特点的基础上，向数百家在华日企提供经营建议(人事劳务、债权债务纠纷、合同相关、商标及知识产权等)，M&A、重组、公司清算相关，劳动仲裁、商事诉讼等全面的法律支持。