# 《个人信息保护法》对资产管理行业的影响

作者：吕红 | 杨迅 | 陈颖华

《个人信息保护法》("《个保法》")已于 2021 年 11 月 1 日正式生效。这是我国首次在个人信息保护领域进行的综合性立法，无论个人信息是以电子还是纸质方式记录，亦无论个人信息指向客户还是员工，均受到该法的保护。《个保法》向个人信息处理者施加了更为严格的个人信息规则，并因此对包括资产管理行业在内的各个行业产生了重大影响。

## 一. An Introduction to PIPL《个保法》介绍

《个保法》起草伊始并非一片空白。《个保法》的诞生不仅反映了我国自 2017 年《网络安全法》生效以来的个人信息保护实践，也同时解决了个人信息保护领域长期存在的部分争议问题，是个人信息保护领域的立法里程碑。

在信息技术被广泛应用前，中国法律并没有明确界定"个人信息保护"。随着个人信息日益成为企业的重要资产，而个人信息的滥用亦可能造成越来越巨大的损失，"个人信息保护"受到了越来越多的关注。

中国关于个人信息保护的立法源起于 2009 年，刑法上将窃取和出售个人信息认定为刑事犯罪。2012 年，全国人大常委会发布《关于加强网络信息保护的决定》，工业和信息化部("**工信部**")据此制定了《电信和互联网用户个人信息保护规定》。2014 年，《消费者权益保护法》加入了关于保护消费者个人信息的条款。2017 年，《网络安全法》规定了关于个人信息保护的原则性规定，这也极大提高了公民个人信息保护的意识。而 2021 年生效的《民法典》更是对个人信息的保护予以专章规定，确认了个人信息为人格权益的组成部分，自然人的个人信息受法律保护。

For more Llinks publications, please contact:

Publication@llinkslaw.com

如您需要了解我们的出版物，请联系:

Publication@llinkslaw.com

上述所有法律法规均现行有效，且基于不同法律关系、从不同视角规范个人信息的保护。尽管《个保法》已经生效，但这些规定仍可适用于个人信息的处理活动。例如，基金个人投资者的信息如通过移动客户端收集和传输的，那么这些信息将被视为互联网用户的个人信息，应遵守工信部《电信和互联网用户个人信息保护规定》的要求。

相应地，《个保法》下履行个人信息保护职责的监管部门涉及多方，该等政府部门将在各自职责范围内负责个人信息保护和监督管理工作。就资产管理行业而言，除行业监管机构(如中国证监会、中国银保监会)结合行业特点对个人信息保护作出相关规定外，国家互联网信息办公室(“**网信办**”)及其地方机构将是《个保法》的核心执法机构。此外，国家市场监督管理总局(“**市监局**”)及其地方机构将从金融消费者权益保护角度、国家安全部(“**国安部**”)及其地方机构将从网络安全角度、工信部将就通过门户网站、手机应用软件或其他公共网络收集或处理个人信息等方面各自履行《个保法》下的监管职责。

值得一提的是，法律责任方面，个人信息处理者违反《个保法》处理个人信息或未履行个人信息保护义务的，情节严重的，将可能面临行政机关高额的罚款。因此，违反《个保法》，个人信息处理者可能承担行政责任和民事责任，构成犯罪的，将被依法追究刑事责任。

## 二. 与资产管理行业的相关性

《个保法》在个人信息保护方面制定了全面且严格的规定。由于资产管理业务涉及处理大量的投资者个人信息，因此《个保法》的要求将影响未来具体业务场景的设计。特别地，资产管理行业应当重点关注《个保法》关于个人信息保护的下列具体内容:

(1) 首先，《个保法》规定了一系列处理个人信息的合法基础。除了长期以来被一致认为是处理个人信息的必要前提“告知、同意”之外，《个保法》首次在国家立法层面拓宽了处理个人信息的合法基础，例如为履行必要的合同义务、法定义务而进行处理的，也被视为处理个人信息的合法基础。在资产管理行业，资产管理机构需要收集的部分个人信息系为提供资产管理服务或为履行法定职责或法定义务所必需。因此，资产管理机构可以考虑依赖该等法律依据减轻落实“告知、同意”方面的负担。

(2) 《个保法》针对敏感个人信息的处理规则予以特别规定。例如，处理敏感个人信息必须取得相关个人的单独同意，并且必须遵从“特定目的”、“充分必要性”及“严格保护措施”的条件。资产管理机构，特别是公募领域，围绕金融账户、身份识别、投资者适当性等方面需要处理海量敏感个人信息，因此必须对这些要求加以关注。

(3) 与欧盟《通用数据保护条例》相似，《个保法》授予了个人对其个人信息的处理享有一定权利。这些权利包括查询、复制、更正、补充、删除其被处理的个人信息、撤回处理个人信息同意，以及指定转移其个人信息。鉴于资产管理机构保留大量客户的个人信息，为应对个人行使权利而建立的相应机制及其具体执行，将可能大大增加机构的运营成本。

(4) 《个保法》将“过错”的举证责任转移给了被告，即个人信息处理者，因此侵犯个人信息权益的行为认定将更为容易。换言之，在个人信息受侵害的情况下，如果个人信息处理者不能证明自己没有过错的，其将视为有“过错”而承担相应的侵权责任。这就要求资产管理机构必须完善并有效实施其关于个人信息保护的相关制度，否则将难以“自证清白”。

## 三. 资产管理行业应对《个保法》需规范的业务场景

资产管理行业可能需要根据《个保法》的要求在以下业务场景中改进个人信息处理的操作:

### 1. 个人单独同意的获取以及个人信息处理规则的公开

“知情同意”并非《个保法》的新创，但是《个保法》对如何获得知情同意提出了更为完整和严格的要求。

2017 年的《网络安全法》第四十一条已明确：网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围。2019 年 1 月 23 日，网信办、工信部、公安部、市监局四部委启动 App 违法违规收集使用个人信息专项治理，其中，将“未公开收集使用规则”列为重点关注的侵害用户权益的违法违规行为。其后，针对专项治理工作，四部委于 2019 年 11 月 28 日联合发布《App 违法违规收集使用个人信息行为认定方法》，明确在 App 首次运行时应通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则，隐私规则不得出现难以访问、难以阅读的情形。2020 年发布的《信息安全技术 个人信息安全规范》更是提供了个人信息保护政策的模版供市场机构参考。《个保法》则进一步明确了寻求个人同意的知情的范围(即告知义务)以及对处理敏感个人信息、向其他个人信息处理者提供个人信息和个人信息出境等的单独同意义务。

因此，目前大部分资产管理机构的网站、App 等金融交易平台已根据上述规定嵌入了个人信息保护政策[1]，该政策在很大程度上落实了应公开个人信息处理的范围、目的和方式的要求。除了对照《个保法》对个人信息保护政策予以更新外，以下三方面涉及资产管理行业的特殊性需充分关注:

(1) 如何落实个人单独同意环节

对于资产管理行业，特别是公募领域，其对于个人信息的处理往往不限于履行其法定职责或法定义务，资产管理机构出于提高其服务质量、获客率、有针对性地开展后续产品推荐等目的，对于个人金融账户持仓特征、购买情况、账户盈亏情况等予以加工分析，甚至通过大数据技术手段对特定类型的客户做群体分析，不仅有利于提高后续资产管理服务的质量，也为监管机构的后续政策制定提供决策依据。如上所述，该等个人信息的处理行为应属敏感个人信息的处理，需

[1]目前行业内对于该政策大多参考海外做法命名为“隐私政策”。但值得注意的是，我国《民法典》第四编人格权下的第六章将隐私与个人信息区别为不同的客体予以民事保护，而机构为落实个人信息保护制定的规则政策仅涉及个人信息处理，并不包括《民法典》下的个人隐私保护，故我们建议可考虑将“隐私政策”调整为“个人信息保护政策”。

要个人的单独同意，且其告知内容区别于一般个人信息，个人有权拒绝资产管理机构的该等处理，亦可撤回同意，资产管理机构不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供金融产品或服务。

而对于单独同意的模式，参考国家标准化管理委员会于 2021 年 5 月 14 日发布的《信息安全技术 个人信息告知同意指南(征求意见稿)》，单独同意是指对于某类具体的业务功能或特定目的的个人信息处理活动，**通过增强式告知或即时提示等方式**，单独向个人信息主体告知处理个人信息的目的、方式和范围、以及存储时间、安全措施等规则，并由个人信息主体明示同意，**单独同意过程不应捆绑与被同意事项不相关的任何业务功能或处理目的**。

因此，针对需要个人单独同意的信息处理活动，如何嵌入单独同意模块、告知的内容范围如何制定以及个人拒绝或撤回单独同意后对于后续信息处理的影响变化均应在本次规范中予以重点考虑。

(2) 如何获取代销客户的单独同意

对于直销客户，即便需要综合考量客户体验、系统改造成本以及对后续数据加工分析的实现等因素对业务的影响，但总体而言，资产管理机构尚可实现在业务场景中加入规则公示/告知、获得个人同意等模块。但是对于无法直接接触的代销客户，资产管理机构如仍考虑将代销客户的金融账户信息纳入大数据统计分析，而合作机构无法或者不愿意提供必要协助的，该等处理活动将因缺少个人的单独同意而无法实现。

诚然，因业务模式的复杂性及个人信息处理目的的多样性及可变性，在资产管理合同等法律文件中大幅加入个人信息保护政策并不符合经济效率原则，一旦个人信息保护政策需更新，将涉及资产管理合同的修改，程序较为复杂，所以我们并不建议将个人信息保护政策或需要单独同意事项“一股脑”地列入资产管理合同并设置单独勾选等模式以实现个人单独同意的获取。但是，对于没有其他直接“连接点”的代销客户，可能需要考虑将个别特殊事项纳入资产管理合同、产品资料概要等个人需签署的法律文件，以充分“调动”各种业务环节，防范法律及行政监管风险。

(3) 机构投资者信息中的个人信息不容忽视

《个保法》下所保护的信息为自然人的个人信息。资产管理机构所处理的大部分机构客户信息均不属于个人信息，一般纳入数据安全的规范范畴。但是，需要注意的是，与机构投资者建立业务关系，因订立合同目的或为履行客户身份识别义务，资产管理机构需要收集法定代表人信息、受益所有人信息以及经办人信息，该等信息属于个人信息，故在与机构投资者业务场景下仍应关注个人信息处理涉及的处理规则告知，甚至在特殊情形下涉及个人同意环节。

## 2. 合作机构管理

《个保法》规定了个人信息转移的多种场景，包括个人信息的对外提供和个人信息的委托处理等。对于不同场景有着不同的个人信息保护要求。资产管理业务链条复杂，投资者信息往往涉及多方根据不同场景的处理，业务生态链上任一环节出现问题，都可能导致资产管理机构承担相应的责任，故如何防范第三方机构风险也是目前资产管理行业落实《个保法》时面临的难题之一。从投资者个人信息保护维度而言，资产管理机构的合作方可分为两类，一类是涉及个人信息处理的机构，如代销机构、登记机构及其他个人信息处理的合作机构。另一类则是，其他可能接触个人信息但不涉及信息处理的普通机构。对于后者的管控，主要关注个人信息传递的合法性，如证券基金领域，根据中国证监会《证券基金经营机构信息技术管理办法》的规定，信息技术服务机构不得截取、存储、转发和使用客户信息。因此，资产管理机构与信息技术服务机构的合作，需保证不得与该等机构存在客户个人信息的交互。

而针对与个人信息处理机构的合作，资产管理机构需特别关注《个保法》等法律法规、国家/行业标准下对于个人信息传输、个人信息共同处理、个人信息委托处理、提供个人信息的相关规定。对于每一类个人信息处理场景，前置程序、信息传递方与信息接收方的权责分工以及与个人信息主体的关系(是否需要获得同意)均有所不同，故对于该等合作机构的管理，应首先厘清与合作机构在个人信息处理过程中的法律关系，即属于委托处理、提供还是共同处理，甚至是否涉及两类以上法律关系的竞合。如资产管理机构与代销机构之间，代销机构将反洗钱涉及的身份信息提供给资产管理机构，属于个人信息的提供，如果属于履行“法定职责或法定义务所必需”，则无需个人的单独同意，但如果其提供的信息超越“法定”范围，如共享个人画像信息，则需要个人的单独同意；此外，如果资产管理机构根据其业务要求委托代销机构获取更多的身份信息(如核查是否为美国人士)，则还同时涉及信息的委托处理。

在厘清各项处理目的背后的法律关系后，资产管理机构应根据法律规定相应设置不同的影响评估程序、明确双方的权责划分以及实施不同的防泄漏信息技术手段等措施以切实履行个人信息保护义务。

## 3. 个人信息出境管理

除了通过投资境内品种实现资产管理以外，资产管理机构在获得特定资质后可通过 QDII、QDLP、QDIE 等机制投资境外品种，为客户配置海外资产。对于该等境外投资，可能涉及海外机构为履行其当地的反洗钱、制裁名单监控等义务，要求境内资产管理机构提供其底层投资者的个人信息。

就此应注意，根据《个保法》第三十八条规定，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：(一)依照《个保法》第四十条的规定通过国家网信部门组织的安全评估(即适用于机构被认定为关键信息基础设施运营者或处理个人信息达到国家网信部门规定数量)；(二)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; (三)按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务; (四)法律、行政法规或者国家网信部门规定的其他条件。

2021 年 10 月 29 日，国家互联网信息办公室发布《数据出境安全评估办法(征求意见稿)》，根据该征求意见稿，“处理个人信息达到**一百万人**的个人信息处理者向境外提供个人信息”及“**累计**向境外提供超过**十万人以上个人信息**或者**一万人以上敏感个人信息**”需要通过所在地省级网信部门向国家网信部门申报数据出境安全评估。除此之外，目前《个保法》提及的专业机构认证及标准合同等配套规则及合同版本亦未落地。

此外，个人信息的跨境提供需在向第三方提供个人信息的基础上，附加适用针对跨境提供的个人信息影响评估、特殊的“告知+同意”程序、对境外接收方的管控，以及限制向外国司法或者执法机构提供个人信息等要求。

## 四. 资产管理机构落实《个保法》的合规建议

随着《个保法》的正式生效，针对资产管理行业的特殊性，我们建议:

### 1. 依法建立并完善个人信息保护相关的内部机制

结合《数据安全法》和《个保法》的要求，资产管理机构应建立相应的个人信息治理机制，包括但不限于:

a) 建立包括个人信息在内的全流程数据安全管理制度;
b) 制定根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等个人信息收集、使用及其相关活动的工作流程和管理制度;
c) 在数据分类分级的基础上，对个人信息实行分类管理;
d) 按照“最小须知”原则管理个人信息处理的操作权限;
e) 针对 i)处理敏感个人信息; ii)利用个人信息进行自动化决策; iii) 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息; 以及 iv)向境外提供个人信息等对个人权益有重大影响的个人信息处理活动，建立个人信息影响评估机制;
f) 建立便捷的个人行使权利的申请受理和处理机制;
g) 梳理个人信息跨境提供需求并相应建立个人信息出境管理制度;
h) 完善合作机构管理制度; 以及
i) 将个人信息处理活动纳入公司应急管理、合规审计的范围。

### 2. 完善个人信息保护政策、增设单独同意模块

通过适当方式予以公开个人信息保护政策及获取个人同意的记录是资产管理机构未来应对侵犯个人信息权益纠纷、“证明自己没有过错”的重要证据，同时也是主管部门检查行业机构是否切

实履行个人信息保护的关注重点之一。资产管理机构应当根据行业特点、实际业务情况、与客户的信息交互模式等制定贴合行业实践的、用于线上线下业务的个人信息保护政策，并优化个人单独同意的模块设计。

**3. 加强合作机构管理**

为有效防范个人信息处理过程中的第三方机构风险，确保机构自身不应第三方机构个人信息处理的违法违规而遭受牵连。根据相关规定，资产管理机构应加强合作机构尽职调查、事中/事后监督评估以及与合作机构在个人信息处理中的权责划分。根据具体的合作模式及各种信息处理活动所涉及的真实法律关系，落实相应的安全措施。同时，根据合作机构的配合程度，督促相对方尽快签署关于个人信息处理的相关安排，明确双方的权利义务及法律责任。

如您希望就相关问题进一步交流，请联系：

吕 红
+86 21 3135 8776
Sandra.lu@llinkslaw.com

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

陈颖华
+86 21 3135 8680
tracy.chen@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

| 上海 | 北京 | 深圳 |
| --- | --- | --- |
| 上海市银城中路 68 号<br>时代金融中心 19 楼<br>T: +86 21 3135 8666<br>F: +86 21 3135 8600 | 北京市建国门北大街 8 号<br>华润大厦 4 楼<br>T: +86 10 8519 2266<br>F: +86 10 8519 2929 | 深圳市南山区科苑南路 2666 号<br>中国华润大厦 18 楼<br>T: +86 755 3391 7666<br>F: +86 755 3391 7668 |
| 香港 | 伦敦 | |
| 香港中环遮打道 18 号<br>历山大厦 32 楼 3201 室<br>T: +852 2592 1978<br>F: +852 2868 0883 | 1/F, 3 More London Riverside<br>London SE1 2RE<br>T: +44 (0)20 3283 4337<br>D: +44 (0)20 3283 4323 | |

**www.llinkslaw.com**

**Wechat: LlinksLaw**

**本土化资源 国际化视野**

免责声明：
本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2021