当信息化遇上保险中介机构
-简评《保险中介机构信息化工作监管办法》

作者：杨迅 | 杨坚琪

2021 年 1 月，中国银行保险监管委员会(**"银保监会"**)对外发布了《保险中介机构信息化工作监管办法》(**"《监管办法》"**)，旨在解决保险中介机构在"触网"过程中存在的"信息化治理不完备、信息系统建设不规范、信息安全机制不健全"等网络安全问题。此外，银保监会的官员在评论《监管办法》时表示，网络系统安全、个人信息保护等要求亦是未来对保险中介机构"信息化"合规工作监管中的重点关注问题。本文将简要解读《监管办法》对保险中介机构(包括保险专业代理人、保险兼业代理人、保险经纪人和保险公估人，以及上述机构的分支机构)提出的具体要求。

第一部分 网络安全要求

近些年来，随着信息技术在金融领域日渐广泛应用，由此引发的网络安全问题也毫无疑问成为金融行业监管的重点之一。无论是公募基金、期货业还是银行业，主管部门都在不断加强对于金融机构的网络安全要求。在此背景之上，《监管办法》则进一步在从"技术、管理和法律"多个维度上，对保险中介机构利用信息技术从事保险中介业务提出了网络安全相关的要求。

(一) 技术要求

《监管办法》从技术方面提出的网络安全要求包括:

首先，《监管办法》要求保险中介机构的储存业务有关数据和客户个人信息的系统应当独立运行，与其他系统，尤其是关联企业的系统有效隔离。《监管办法》第 8 条指出，保险中介机构应当保持**"重要信息机制、设施和其管理"**的独立完整，并与其关联企业(含股东、参股企业和其他类型的关联企业)的相关设施进行**"有效隔离"**，以防止关联企业违规自保险中介机构处获取保单、个人信息等数据信息。《监管办法》的第八条特别提及，**"业务、财务、人员等重要信息系统**

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

以及其中的数据信息”属于**“重要信息化机制、设施”**。根据本条的要求，保险中介机构需要自查目前的信息技术系统的实际使用情况，包括自研系统、集团内共用系统以及采购“云服务”的情况，**并检查“隔离措施”(包括物理隔离和逻辑隔离)是否具备满足监管要求的有效性**。

其次，《监管办法》第 17 条和第 21 条对保险中介机构的业务、财务和人员管理信息系统应当具备的功能提出了一系列功能性要求:

	信息系统	具体要求
1	业务管理系统	• 能够记录并管理业务协议、保险业务详细情况、客户信息、相关凭证和其他业务情况等 • 业务管理系统的数据能够与财务管理系统和人员管理系统的数据匹配一致，且具备互相验证的功能 • 能够生成符合监管要求的数据文件，且能够通过技术手段直接与监管相关的信息系统实现对接 • 具备必要的用户权限分级机制，为不同角色的用户设定增删、修改、查看和访问权限 • 具备日志管理功能，能够记录用户操作行为和时间 • 应在各保险业务环节发生之日起 3 个工作日内，录入相关的数据，如同时涉及财务、人员事项应同步完成财务和人员明细数据录入
2	财务管理系统	• 能够记录并管理财务总账、科目明细账、应收应付、会计报表、发票等 • 财务管理系统的数据能够与业务管理系统和人员管理系统的数据匹配一致，且具备互相验证的功能 • 能够生成符合监管要求的数据文件，且能够通过技术手段直接与监管相关的信息系统实现对接 • 具备必要的用户权限分级机制，为不同角色的用户设定增删、修改、查看和访问权限 • 具备日志管理功能，能够记录用户操作行为和时间
3	人员管理系统	• 能够记录并管理保险中介从业人员的基本信息、入职离职、用工合同、执业登记、人力薪酬、培训和奖惩等情况 • 人员管理系统的数据能够与业务管理系统和财务管理系统的数据匹配一致，且具备互相验证的功能 • 能够生成符合监管要求的数据文件，且能够通过技术手段直接与监管相关的信息系统实现对接 • 具备必要的用户权限分级机制，为不同角色的用户设定增删、修改、查看和访问权限 • 具备日志管理功能，能够记录用户操作行为和时间

4	其他与信息系统相关的要求	• 能够与合作保险公司的系统实现互通、业务互联、数据对接的需求 • 能够根据合作机构、分支机构、业务类别、业务渠道、险种、收支口径、区域、时间等维度，对保险中介机构的经营情况进行回顾 • 满足相关的行业标准和技术规范

再次，《监管办法》还要求保险中介机构履行网络安全等级保护义务，为机构使用的各类电子设备(例如计算机、智能手机等)设定安全措施。《监管办法》的第 24 条要求保险中介机构为其信息系统进行合理定级，按照相应等级采取防护措施，以获取相应的国家网络安全等级保护认证。通常而言，持牌金融机构的用以为公众开展金融服务的信息系统，由于其储存和处理用户个人信息，定级通常不会低于三级。

此外，《监管办法》第 27 条对计算机、智能手机、平板电脑等终端设备的安全性提出了要求，保险中介机构应当采取包括但不限于登录控制、病毒防护、软件安装与卸载管理、移动存储介质管理、固定资产管理、网络准入、违规监测等措施以维护终端设备本身的安全性。

(二) 管理要求

除了技术维度之外，《监管办法》还对保险中介机构的网络安全管理制度提出了具体且具有可执行性的规定，包括:

- 指定一名高级管理人员负责保险中介机构(包括其分支机构)的信息化工作，高级管理人员包括但不限于公司总经理、公司副总经理、首席信息官等;
- 保险中介机构应当具有专门负责信息化的部门，且该部门中的正式工作人员不得少于一人;
- 保险中介机构应当设立信息安全管理制度，部署实施边界防护、病毒防护、入侵检测、数据备份、灾难恢复等信息安全措施(以及其他《监管办法》要求的技术措施)，以保证业务连续性;
- 保险中介机构应当定期开展信息化培训、信息安全培训和保密教育，与员工签署必要的保密协议，增加员工的信息安全和保密意识。

在上述的管理要求之外，呼应《数据安全法(草案)》中对于数据安全保护，《监管办法》第 25 条还特别要求对保险机构的**重要数据**采取必要的“保护措施”，以保证重要数据处理全流程安全，严防数据泄露、篡改或者损毁。同时，《监管办法》还要求保险中介机构采取数据备份措施，并定期开展数据恢复验证: 其中，系统数据应当至少保存五年，而系统日志数据不得存储低于 6 个月。

(三) 法律要求

《监管办法》重申了软件正版化要求。使用正版软件不仅是知识产权法律的要求，也是避免被责令停止使用，或失去软件支持服务带来的系统风险的有效举动。《监管办法》第 15 条特别指出: 要求保险

中介机构“使用正版软件，禁止复制、传播或使用非授权软件”。在此要求下，保险中介机构应当尽快核实和确认自身的软件资产，在必要的情况下尽快采取整改措施。

此外，银保监意识到大型的保险中介机构也在不断加强自身的信息技术实力(无论是自行研发还是通过和第三方合作完成研发)，创新的信息技术应用层出不穷。 正是基于这样的现实情况，《监管办法》第 15 条还要求保险中介机构对具有“自主知识产权的信息系统”采取有效措施加以保护，常见的保护措施有进行软件著作权登记、制定企业内部的商业秘密保护制度防止源代码非法披露等。

第二部分 个人信息保护要求

随着个人信息的经济价值被不断发掘，以及社会各界对个人信息的认识提高，个人信息保护已经俨然成为各行各业都在不断强调和重视的法律要求。《网络安全法》、《民法典》以及《个人信息保护法(草案)》等多部重要的法律都对个人信息的保护做出了全面而细致的规定。与之相对应的，保险中介行业具有自然人客户数量众多，涉及个人信息种类较为敏感，以及个人信息流动频繁等特点。据此现状，《监管办法》作为保险中介行业信息化工作的“纲领性文件”，对保险机构的个人信息保护工作提出了要求。

首先，是“信息隔离”要求。《监管办法》第 8 条要求保险中介机构不能“违规向关联企业泄露保单、个人信息等数据信息”，这表明原则上保险中介机构不能**直接**与关联企业披露保单以及客户的个人信息等数据信息。在实践中，为了增加业务的统一性，保险中介机构往往会选择使用关联企业提供的统一信息系统对外提供服务。而关联企业集团为了方便业务的进行，关联公司通常也会被允许访问保险中介机构获取的客户的保单、个人信息等数据或信息。在《监管办法》第 8 条出台之后，这样的实践模式直接存在“合法性”风险，保险中介机构应当慎重考虑是否需要继续使用这种商业模式。

其次，个人信息处理全流程合规性要求。《监管办法》第 26 条要求保险中介机构在收集、处理和应用个人信息时，应当满足“合法、正当和必要”原则，遵守国家相关法律、行政法规(包括《民法典》和未来生效的《个人信息保护法》)的要求；在此基础之上，《监管办法》还特别提出要求**遵守“与个人信息安全相关的国家标准”的要求**。直接援引国家标准作为法律要求在行业立法中并不常见。在目前众多与个人信息安全相关的国标中，《信息安全技术-个人信息安全规范》毫无疑问是最重要也是最为详尽的一部国家标准，对个人信息保护工作提出了详实的合规要求。因此，鉴于《监管办法》的规定，保险中介机构应当尽快启动“合规校准”工作，以保证目前公司内部的管理制度和技术手段符合国标中个人信息的保护尺度。

最后，《监管办法》还特别对于保险业中的**常见的个人信息“违规行为”**进行了列举式的说明。《监管办法》第 26 条特别指出了如下个人信息违规行为:

- 保险中介机构收集与**保险中介机构提供服务无关的**个人信息;
- 违反法律规定和**合同约定**收集、使用、提供和处理个人信息;
- **泄露、篡改**个人信息。

根据上述的要求，我们建议保险中介机构核实: 1)目前的个人信息收集的具体范围, 2)对外提供个人信息的对象；以及 3)目前企业内部对于个人信息相关的权限管理制度，以确认是否符合《监管办法》第 26 条的规定。

第三部分 外包管理要求

信息技术的服务外包，有助于企业集中关注核心业务。采用先进和专业的信息服务，以及降低信息化建设的成本，是保险中介业务，乃至金融行业的重要的组成部分。《监管办法》对此也提出了安全方面的要求。

第一，《监管办法》的第 18 条明确允许保险中介机构可以采取**各类方式**建设信息系统，包括自主开发、合作开发、定制开发、外包开发和购买云服务等。换而言之，银保监在选择信息系统的建设方式上，给与保险中介机构充分的自主性。根据《监管办法》现有的规定，如果保险中介机构的规模较小，那可以选择采购各种类型的商业化云系统以满足成本要求；如果保险中介机构自身具备一定的技术实力，也可以选择自主开发的形式完成信息系统的建设。从《监管办法》体现的监管态度来看，银保监会对金融科技的应用秉持的是“兼容开放”态度。

第二，《监管办法》提出了对外包服务商的尽职调查要求。虽然《监管办法》允许保险中介机构自行选择信息系统的建设方式，但是如果中介机构选择与外部合作方式完成的，则中介机构仍然需要履行尽职审核义务。《监管办法》第 19 条规定，在选择利用外部力量建设信息系统的情况下，中介机构应当完成如下的审核义务:

- 审核外包服务商是否具备必要的资质，包括技术能力资质和业务资质;
- 审核是否签署包含必要条款的外包合同，合同条款中应当含有双方在外包合作中的权利义务关系、保密责任和**个人信息保护责任**;
- 审核合作建设的信息系统是否足够安全，且能够满足业务连续性的要求。

尤为值得注意的是，《监管办法》特别规定，**即使是将信息系统建设的任务交给关联公司的，保险中介机构的审核义务也不会因关联关系而变化**。

第三，《监管办法》提出了信息服务外包的安全管理要求。《监管办法》要求: 在正式启动合作开发的信息系统前，保险中介机构: 1)开展风险评估, 2)编制实施计划和应急处置方案, 3)进行必要的测试和培训，以减少或者避免信息系统变更导致的业务风险。同时，在信息系统正式上线后，保险中介机构还应当组织有效性验证，以确认正式上线后的信息系统能够符合《监管办法》的要求。

最后，《监管办法》对信息服务外包过程中的个人信息保护提出要求。由于在信息系统外包或者采购云服务的过程中，不可避免的会涉及到客户个人信息/数据对外传输的问题，因此，《监管办法》要求保险中介机构需要重视外包过程中的个人信息保护，例如考虑如下问题:

- 是否在个人信息保护声明等文件中向客户充分披露对外披露的情况并征求客户的同意;

- 是否进行个人信息风险评估，以确认外包过程满足个人信息保护要求；
- 是否在合同中存在必要的条款，以确认满足《监管办法》的需求。

第四部分 “前、中、后”全程监管

《监管办法》严格地在“前、中、后”端全面监管保险中介机构的信息化工作。

在“前端”，《监管办法》要求保险中介机构在开展信息化建设后，向**“机构营业执照登记注册地银保监会派出机构报送信息化工作情况报告”**，工作情况报告中应当包括：1)信息化管理机制和制度完善情况；2)信息系统具备《监管办法》第 17 条列明功能的证明；3)信息系统采购合同或知识产权证书；以及 4)其他监管部门要求报告的内容。此外，保险中介机构如果需要设立分支机构的，还应当依照《监管办法》的要求向分支机构营业执照登记注册地银保监会派出机构报送**法人机构及其分支机构的信息化工作情况报告**。

在“中端”，《监管办法》则要求保险中介机构一旦发生“信息化突发事件”，应当按照“银保监会信息化突发事件信息报告相关规定”(如《银行业保险业突发事件信息报告办法》)在 **24 小时**内向机构营业执照登记注册地银保监会派出机构报告。但如果“信息化突发事件”属于“特别重大、可能造成严重社会影响”的事件，则保险中介机构应在 **30 分钟内电话报告相关信息、1 小时内书面报告相关信息**。《监管办法》下“信息化突发事件”指的是：

- 信息系统或信息化基础设施出现故障、受到网络攻击，导致保险中介机构在同一省份的营业网点、电子渠道**业务中断 3 小时**以上，或在两个及以上省份的营业网点、电子渠道业务中断 **30 分钟**以上；
- 因网络欺诈或其它信息安全事件，导致保险中介机构或客户资金损失 **1000 万元**以上，或造成重大社会影响；以及
- 保险中介机构**丢失或泄露大量重要数据或客户信息**等，已经或可能造成重大损失、严重影响。

在“后端”，《监管办法》的第 31 条规定，一旦监管部门发现“保险中介机构信息化工作不符合本办法要求的”，**保险中介机构将被禁止经营保险中介业务**，法律后果可谓严厉。

结语

《监管办法》体现了银保监会对于保险中介机构有关信息技术工作的监管态度：即鼓励保险机构们利用“信息化”技术改造保险中介业务，但是同时注意科技风险，并保持与监管部门的有效沟通。

《监管办法》第 34 条特别给与保险中介机构**为期 1 年的合规整改期限**，则反映了监管部门务实的监管策略，而这也表示在期限过后，监管的大闸必将落下。因此，无论是在《保险代理人监管规定》出台之前已经设立的保险代理机构和保险经济机构，还是在《保险代理人监管规定》出台之后的新兴的保险代理机构(尤其包括保险兼业代理机构)，都应当对《保险中介机构信息化工作监管办法》对信息化提出的监管要求予以足够的重视，利用一年的合规整改期限重审自身网络安全和个人信息保护实践，及时纠正不符合法律要求的信息系统和信息化操作。

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@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 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野