君合专题研究报告 JUNHE

2022 年 02 月 24 日

互联网保险合规专题系列文章（五）：互联网保险业务存在的主要问题、风险及合规应对——个人信息保护（上）

引言

互联网保险业务的业务性质决定了其需要面临和处理复杂的数据合规问题。保险业务往往涉及多方自然人的个人信息，如投保人、被保险人、受益人；又常常涉及敏感个人信息（个人金融信息、个人健康信息等），同时，互联网保险业务相比传统保险业务，还可能涉及通过网站、手机 App 等方式收集的用户行为数据。因此，当我们讨论互联网保险合规时，数据合规是不可回避的重要议题。

君合保险团队将携手数据合规团队，共同对互联网保险领域项下个人信息保护的监管规定及合规问题予以介绍。

一、 概述

互联网保险业务是保险机构依托互联网和移动通信等技术，通过自营网络平台、第三方网络平台等订立保险合同、提供保险服务的业务。其之所以复杂，是因为其结合了保险行业及互联网业务模式的双重特征。

就保险行业而言，保险机构作为银保监会监管下的金融机构，保险业务涉及社会民生，自然决定了其强监管的特征；而就互联网业务模式而言，信息的生产（收集）、聚合、处理和分发是网络运营业务的本质。此外，由于互联网保险业务涉及的保险产品既有传统业务中常见的健康险、财产险、意外险等产品，也有在互联网场景中发展出的如延误险、运费险等新种类，因此，基于业务需求，无论是保险机构还是其合作的非持牌机构均不可避免地收集和处理数量较大、种类多样、内容涉敏的个人信息。互联网保险业务基于该等保险行业和互联网业务模式的双重性，对于客户个人信息的管理，既需要符合行业监管机关对保险业务客户信息真实性管理等既有监管要求，也需要符合互联网业务数据和客户个人信息保护的一般要求。

如我们在本系列之前文章中所述，伴随着互联网保险业务规模的日渐壮大，与互联网有关的风险同样蔓延到了互联网保险领域，在网络安全、数据安全及个人信息保护立法及实践不断加深加强的监管背景下，如何在业务发展与业务合规之中找到一个平衡点，将成为所有互联网保险业务参与主体需要审视及思考的问题。对此，我们就互联网保险业务的监管规定、合规要点进行了梳理。

二、 监管规定梳理

适用于互联网保险业务个人信息保护的规定包括但不限于《中华人民共和国个人信息保护法》（简称“**《个保法》**”）、《中华人民共和国网络安全法》（简称“**《网安法》**”）、《中华人民共和国数据安全法》（简称“**《数安法》**”）、《儿童个人信息网络保护规定》、《关键信息基础设施安全保护条

例》（“简称**《关基条例》**”）、《App 违法违规收集使用个人信息行为认定方法》、《常见类型移动互联网应用程序必要个人信息范围规定》、《互联网保险业务监管办法》（简称“**《互联网保险办法》**”，银保监会令 2020 年第 13 号）、《保险中介机构信息化工作监管办法》（简称“**《保险中介信息化办法》**”）、《金融数据安全 数据安全分级指南》、《金融数据安全 数据生命周期安全规范》、《个人金融信息保护技术规范》、《信息安全技术 个人信息安全规范》（GB/T35273-2020）等法律、法规及国家标准。

三、 合规要点剖析

相较于一般企业，保险机构开展互联网保险业务，在数据合规、网络安全等方面首先需要关注的是其在互联网保险业务开展过程中的角色及需要承担的特别责任。然而，在互联网保险业务开展过程中，保险机构是否可能构成关键信息基础设施的运营者，是一个尚未有明确结论的问题。

《网安法》第 31 条规定，国家对公共通信和信息服务、能源、交通、水利、**金融**、公共服务、电子政务等重要行业和领域，以及其他**一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施**，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

《关基条例》第 2 条则规定，本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、**金融**、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他**一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统**等。

由于“金融”属于上述定义中列举的关键行业之一，我们无法排除保险机构落入关键信息基础设施运营者范围的可能性。但是否达到以上条款中描述的后果标准，我们理解，每个保险机构的情况各不相同。对于客户数量巨大、市场占比额度高、掌握的数据量巨大的保险机构而言，确有可能落入关键信息基础设施运营者的范围中。

另外，根据《关基条例》的规定，相关保护工作部门应根据认定规则负责组织认定本行业、本领域的关键信息基础设施，**并及时将认定结果通知运营者**。因此，是否收到关键信息基础设施的认定通知亦可作为保险机构判断自身构成关键信息基础设施运营者可能性高低的重要依据。

如构成关键信息基础设施运营者，保险机构将承担若干额外的安全义务，具体可参见《关键信息基础设施安全保护条例正式出台》。

另外一个值得关注的问题是，《个保法》第 58 条提出，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，应当履行下列义务：

1、 按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；

2、 遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；

3、 对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；

4、 定期发布个人信息保护社会责任报告，接受社会监督。

保险机构如提供平台级的服务，例如，通

过网络平台展示多家保险公司的产品、把消费者和保险服务、信息、资金等连接起来，使得平台具有资讯、交易等多种功能，有可能落入互联网平台的定义中，并且在其用户数量巨大、经济体量巨大时，有可能落入上述第 58 条的规制范围。2021 年 10 月 29 日，国家市场监督管理总局公开对《互联网平台分级分类指南》和《互联网平台落实主体责任指南》征求意见，其中对超级平台、大型平台、中小平台的分级提供了依据，并规定了超大型平台经营者、互联网平台经营者在数据管理、内部治理、风险评估、数据获取、算法规制、网络安全、数据安全、隐私与个人信息保护等方面的要求。

四、 法律法规对保险机构开展互联网保险业务的特殊要求

（一）适用于所有保险机构的要求

《互联网保险办法》适用于保险公司和保险中介机构；其中保险公司含相互保险组织和互联网保险公司，保险中介机构包括保险代理人（不含个人保险代理人）、保险经纪人、保险公估人。《互联网保险办法》在数据合规、网络安全方面提出的要求主要有：

1、 **合法合规处理个人信息**：收集、处理和应用数据涉及到个人信息的，应遵循合法、正当、必要的原则，遵守国家相关法律、行政法规，符合与个人信息安全相关的国家标准，应征得个人信息主体同意。未经允许或授权，不得收集与其提供的服务无关的个人信息；不得违反法律、行政法规和合同约定收集、使用、提供和处理个人信息；不得泄露、篡改个人信息；不得将客户个人信息用于所提供保险服务之外的用途。（第 38 条）

2、 **明示保护消费者的保障措施**：应在开展互联网保险业务的自营网络平台显著位置列明针对消费者个人信息、投保交易信息和交易安全的保障措施。（第 13 条）

3、 **核心系统和信息管理系统有效隔离**：具有支持互联网保险业务运营的信息管理系统和核心业务系统，应与其他无关的信息系统有效隔离。（第 7 条）

4、 **落实网络安全等级保护**：贯彻落实国家网络安全等级保护制度，对于具有保险销售或投保功能的自营网络平台，以及支持该自营网络平台运营的信息管理系统和核心业务系统，相关自营网络平台的安全保护等级应不低于三级；对于不具有保险销售或投保功能的自营网络平台，以及支持该自营网络平台运营的信息管理系统和核心业务系统，相关自营网络平台和信息系统的安全保护等级应不低于二级。（第 7 条）

5、 **对合作机构要求落实网络安全等级保护、加强合规管理：**对提供技术支持和客户服务的合作机构加强合规管理，督促其保障服务质量和网络安全，其相关信息系统至少应获得网络安全等级保护二级认证。（第 37 条）督促提供技术支持、客户服务等服务的合作机构建立有效的客户信息保护制度，在合作协议中明确约定客户信息保护责任，保障客户信息安全。（第 38 条）

6、 **服务境内接入：**开展互联网保险业务的自营网络平台服务接入地应在中华人民共和国境内。（第 7 条）

7、 **年度报告：**保险机构每年 4 月 30 日前应向互联网保险监管相关信息系统报送上一年度互联网保险业务经营情况报告，其中应包括**网络安全建设**、消费者权益保护和投诉处理、

信息系统运行和故障情况等。（第 74 条）

我们理解，在《网安法》、《数安法》、《个保法》相继生效并要求各主管部门加强对行业内的合规监管、中国人民银行就银行业金融机构已经出台多部相关法律法规、证监会也就相关问题出台了《证券基金经营机构信息技术管理办法》等详细细则要求的背景下，银保监会对于保险机构的信息安全、数据合规的要求也会更为严格和细节。

（二）适用于保险公司的要求

就保险公司而言，有《保险公司开业验收指引》、《保险公司信息系统安全管理指引（试行）》、《保险业信息系统灾难恢复管理指引》等专门的规定，对于保险机构的信息系统建设、信息合规要求有非常具体的标准，在此不进行赘述。

（三）适用于保险中介机构的要求

《保险中介信息化办法》适用于保险中介机构，包括保险代理人（不含个人保险代理人）、保险经纪人和保险公估人，包括法人机构和分支机构。保险代理人包括保险专业代理机构和保险兼业代理机构。

该办法是围绕保险中介机构信息化工作展开的规定，要求详尽具体，主要的要点包括：

1、 **关联企业分离：**应当厘清与关联企业之间的信息化工作职责，各自承担信息安全管理责任。不得违规向关联企业泄漏个人信息。（第 8 条）

2、 **外包明确责任：**采用合作开发、定制开发、外包开发和购买云服务等外包模式建设信息系统的，**应于协议中明确个人信息保护责任**。（第 19 条）

3、 **自主开展信息化：**保险中介机构应自主开展信息化工作。**信息化工作与关联企业（含股东、参股企业、其他关联企业）有关联的，保险中介机构应厘清与关联企业之间的信息化工作职责，各自承担信息安全管理责任。**保险中介机构的重要信息化机制、设施及其管理应保持**独立完整**，与关联企业相关设施**有效隔离**，严格规范信息系统和数据的访问、使用、转移、复制等行为，**不得违规向关联企业泄露保单、个人信息等数据信息。**重要信息化机制、设施包括但不限于信息化治理与规划，业务、财务、人员等重要信息系统及其中的数据信息。（第 8 条）

4、 **信息化突发事件报告：**发生信息化突发事件的，应按照银保监会信息化突发事件信息报告相关规定在 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信息。特别重大、可能造成严重社会影响的信息化突发事件发生后，保险中介机构应在 30 分钟内电话报告相关信息、1 小时内书面报告信息。（第 14 条）

5、 **信息系统的详尽要求：**保险中介法人机构应根据业务规模和发展需要，建立相匹配的业务管理、财务管理和人员管理等信息系统，并符合以下要求：

(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。

(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。

(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。

(4) 业务管理、财务管理与人员管理系统的数据能够匹配一致、相互验证。

(5) 通过技术手段实现与合作保险公司的系统互通、业务互联、数据对接。

(6) 能够生成符合监管要求的数据文件，通过技术手段实现与保险中介监管相关信息系统的数据对接。

(7) 能够按照合作机构、分支机构、业务类别、业务渠道、险种、收支口径、区域、时间等维度对机构经营情况进行汇总和分析。

(8) 具备用户权限管理功能，能够按照不同角色为用户配置数据的增加、删除、修改和查看权限。

(9) 具备日志管理功能，能够记录用户操作行为和操作时间。

(10) 遵循国家标准化管理部门和银保监会发布的相关行业标准和技术规范。（第17条）

6、 权限设计：应按照最少功能、最小权限原则合理确定信息系统访问权限并定期检查核对，确保用户权限与其工作职责相匹配。严格控制系统访问权限，禁止未经授权查看、下载数据。严格控制通过系统后台修改数据，确需修改的要做到事前批准、事中监控和事后留痕。（第20条）

7、 数据安全、存储、备份和备份数据恢复验证：保险中介机构应对重要数据采取保护措施，保障数据在收集、存储、传输、使用、提供、备份、恢复和销毁等过程中的安全，合法使用数据，严防数据泄露、篡改和损毁，保障数据的完整性、保密性和可用性。保险中介机构应采取可靠措施进行数据存储和备份，定期开展备份数据恢复验证。系统数据应至少保存五年，系统日志应至少保存六个月。（第25条）

8、 终端管理：加强对台式计算机、便携式计算机、智能手机、平板电脑、移动存储介质等终端设备的管理，根据法律、行政法规要求和本机构网络安全实际情况对终端设备选择实施登录控制、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、违规监测等安全措施。（第27条）

9、 员工管理：保险中介机构应经常开展信息化培训、信息安全培训和保密教育，与员工签订信息安全和保密协议，督促员工履行与其工作岗位相应的信息安全和保密职责。（第28条）

以上要求中，部分内容属于已有规定的要求；但同时，也有部分内容对保险中介机构提出了特别的要求，包括针对信息系统的独立性、以及与关联公司的切割。该等要求很可能与近年来出现多家互联网企业收购或申请保险中介牌照的现象有密切关联。监管机构不希望这些互联网集团公司利用手中的互联网中介机构牌照大量收集个人金融信息，并与其旗下的其他产品进行打通，绘制用户画像，因此，对于该类保险中介机构而言，信息系统的独立化是其数据合规的重要要件。

此外，对于互联网保险业务开展过程中产生的金融数据的保护亦为时下数据合规领域的热点问题。但是，由于篇幅限制，关于金融数据的特殊合规要求我们将放到下一篇进行详述，敬请各位读者期待！

邓梁　　合伙人　　电话：86 10 85191276　　邮箱地址：dengl@junhe.com
李澍　　律　师　　电话：86 10 85537823　　邮箱地址：lishu@junhe.com