Deloitte.

德勤

创变领航 坚韧致远

保险业个人信息治理破局新攻略

因我不同
成就不凡
始于1845

引言

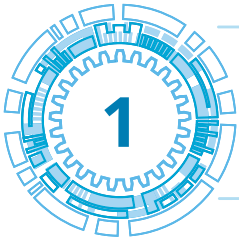
在当今数字化时代，个人信息的保护已成为各行各业亟待解决的重要问题。保险行业作为处理大量敏感个人信息的行业之一，面临着独特的挑战和责任。随着保险科技的快速发展和数字化转型的推进，个人信息的收集、存储和使用变得更加频繁和复杂，也更容易受到安全威胁。

本报告旨在探讨保险行业个人信息保护所面临的难点与挑战，并提出相应的应对策略和思考。首先，报告从监管要求、治理体系、合规共享等方面对个人信息保护形势进行梳理，剖析保险行业中存在的难点与挑战。其次，报告结合业内实践和先进经验，提出在相关领域的思考，并给出应对策略和推进方法。

通过本报告的研究和分析，我们希望能够为保险行业在数字化转型时代的个人信息保护提供有益的参考和借鉴，助力保险机构更好地应对数字化转型时代的个人信息保护挑战。愿本报告能为保险行业的相关从业人提供有价值的信息与洞见。

一、数字化转型时代下保险行业个人信息保护能力建设的难点与挑战

在可持续增长和业务创新的推动下，数字化转型技术将重塑保险行业的各个环节价值链，从而推动保险保障类型、产品内涵、业务模式和行业生态发生根本性的变革。在这个过程中，会涉及大量个人信息加工和应用，而个人信息备受监管部门、保险机构以及数据主体的重点关注，保险机构如何构建个人信息保护体系，符合监管要求、满足自身业务发展需求、响应数据主体权利诉求，对整个保险行业充满了挑战，需要保险行业深入思考探讨，并积极布局应对策略。



1 个人信息保护与业务发展平衡需要更多关注

为了维护保险行业的良好秩序和消费者的合法权益，近年来，国家监管部门和行业协会对保险行业的个人信息保护工作进行了严格的规范和监督。《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《中华人民共和国民法典》《中华人民共和国消费者权益保护法》等法律法规对个人信息的定义、收集、使用、保存、传输等方面都作出了明确的规定。此外，原中国银保监会还制定并发布了《银行保险机构消费者权益保护管理办法》，下发《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知（银保监办法〔2022〕80号）》也旨在规范银行保险机构在收集、使用、存储、传输个人信息等方面的行为，以保护消费者的个人信息安全。

从监管趋势来看，保险行业的个人信息保护监管正朝着更加严格和规范的方向发展。监管机构对保险机构的个人信息处理、使用和披露等方面的要求和指引更加明确、更加精细，对保险机构的个人信息保护安全措施和保护政策提出了更高的要求。

从保险行业总体发展趋势来看，随着保险科技的快速发展和应用，保险行业的业务发展正朝着数字化、智能化和个性化的方向发展，保险机构越来越注重通过数字化渠道来拓展业务。人工智能（AI）、区块链等新技术的应用既加速了保险业务的智能化进程，但也会涉及到一系列的个人信息保护场景。例如，利用AI技术进行智能客服、个性化推荐服务时，可能涉及到年龄、性别、健康状况、财务状况等个人信息的使用；区块链驱动的智能合约可以即时授权支付，但也涉及到客户财务账户信息的访问和使用。此外，随着保险机构国际化进程的加速、高水平的对外开放，越来越多的保险机构拓展海外业务，在业务拓展过程中，保险机构也面临不同国家和地区关于个人信息出境的监管要求。在这些过程中，保险机构如果未能妥善处理和保护好个人信息，可能会存在侵犯个人隐私权益、个人信息泄露以及触犯个人信息跨境监管要求等风险。保险机构在使用上述相关技术和拓展海外业务时，需要特别注意个人信息的保护，确保遵守相关的法律法规，进而提高自身的竞争力和可持续发展能力。

因此，保险机构在面临日益完善和精细的监管要求，以及自身业务快速发展过程中的变化，保险机构在个人信息保护合规与业务快速发展之间如何平衡需要投入更多关注。一方面保险机构需要投入更多资源来跟踪监管趋势和变化，及时实现“外规内化”、完善自身防护能力要求。另一方面保险机构还需要在不断创新业务模式和技术应用过程中，落实这些防护能力要求、加强个人信息保护，避免因技术创新而引发新的合规风险。

个人信息保护治理体系的构建与落地亟待推行

随着保险科技的发展和应用范围的不断扩大，以及保险机构自身在多种业务场景下对个人信息的开发、运用越来越多元化，个人信息保护面临着更多的挑战和风险，为了保障个人信息的合法权益和安全，构建纵向贯穿、横向协同，全方位、多层次的个人信息保护治理模式无疑是个人信息保护重要保障之一，然而这一过程面临诸多影响因素，值得行业深入探讨与思考。

在纵向管理方面，保险机构通常由集团总部、分子公司、区域办事处、营销服务部等多层机构组成。在个人信息保护治理体系设计中，明确不同层级之间的职责和权限至关重要。集团总部应制定个人信息保护政策和策略，监督和管理整个集团的个人信息保护工作。分子公司和区域办事处应执行总部的政策和制度，确保个人信息在本单位的合规使用和管理。营销服务部作为最接近客户的层级，应严格遵循个人信息保护政策，负责收集、处理和存储客户的个人信息，并为客户提供个人信息保护相关的服务和支持。

在横向协同方面，保险机构通常涉及核保、理赔、产品开发、市场推广与销售、客户服务与关系管理、信息科技、风险和合规管理等多个部门。在个人信息保护横向协同方面，不同部门在业务目标上存在差异，业务相关部门致力于推动个人信息的收集和应用，以促进业务的高效运营并提供更为优质的客户服务；科技相关部门专注于技术创新和系统的不断优化，为公司的业务运营提供技术支持；合规相关部门专注于确保业务过程中严格遵循监管要求，以保障公司各项经营活动的合规性。因各自目标的差异性以及各部门之间存在沟通不畅的情况，如何平衡部门间个人信息保护工作并实现业务可持续发展成为保险机构的一个难题。

因此，随着保险科技的发展和保险业务场景的多元化，以及保险机构管理层次复杂、协同业务部门众多，个人信息保护面临更多挑战。构建一套能够贯通上下各组织层级、协同前后各业务环节的个人信息保护治理模式是关键。在纵向贯通方面，保险机构需明确各层级的职责和权限，确保合规使用和管理；在横向协同方面，保险机构需构建跨职能、跨组织的协作机制，指导各部门开展个人信息保护相关活动。

混业经营下的安全流通与合规共享难题

为满足客户日益增长的综合化金融服务需求，保险机构通常通过混合经营模式，将保险产品与其他金融产品或非金融产品进行组合搭配，为客户提供一站式的金融服务。混业经营模式下将集团内部的技术、渠道、人员等资源进行流通、共享，实现优化资产配置，在这过程中个人信息数据也可能被作为一种资源进行整合。

与此同时，国家和地方政府层面持续完善数据流通和共享顶层设计和实施意见。相关政策内容中均会提及在安全合规前提下，发挥数据要素流通和共享相关价值，这为保险机构对个人信息数据要素价值的发挥也明确了底线和要求。1）2022年12月，国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”），提出“建立健全个人信息数据确权授权机制”的相关要求。2）2023年6月，北京市印发《关于更好发挥数据要素作用进一步加快发展数字经济的实施意见》，提出“推进建立个人数据分类分级确权授权机制，允许个人将承载个人信息的数据授权数据处理者或第三方托管使用，推动数据处理者或第三方按照个人授权范围依法依规采集、持有、使用数据或提供托管服务。”3）2023年7月，上海市印发《立足数字经济新赛道推动数据要素产业创新发展行动方案（2023—2025年）》“建立数据分类分级保护制度，制定重要数据目录，严格实施个人信息保护。”因此，在混业经营模式下，个人信息要素在不同业态、不同层级机构下的流通和共享，给保险机构也带来了一些管理难题。

首先，由于个人信息存在特殊性，在个人信息被流通和共享之前，保险机构需要确保客户对个人信息的流通和共享有充分的知情权和选择权，“数据二十条”也提出了不得采取“一揽子授权”或强制同意的方式过度收集个人信息。这意味着保险机构必须明确告知客户其数据将如何被采集、持有、托管和使用，并且在获取客户的明确同意后才能进行相关流通和共享。

其次，个人信息主体还可以主张其他相关权利，如知情权、拒绝权等，例如在个人信息主体申请使用个人信息主体权利进行退保，查阅等服务时，保险机构理应受理个人信息主体的申请，通过平台处理或者人工受理的方式，解决个人信息主体提出的要求，这意味着保险机构在收集、处理和使用这些个人信息时，需要在各个环节保障个人信息主体权利。这对保险机构来说，无疑增加了合规的难度和成本。

最后，个人信息数据作为数据要素流通时，还应在数据分类与权属界定方面提高重视，“数据二十条”提出了数据资源持有权、数据加工使用权和数据产品经营权的“三权”分置的结构性产权制度框架。这就要求保险机构在生产经营过程中，对所控制的个人信息数据进行清晰的分类和权属界定，确保个人信息数据的合法来源和使用。

总的来说，为了在混业经营模式下，实现个人信息数据安全流通、合规共享，不仅需要考虑保险机构自身的管理规范和技术措施，还需要提高对个人信息主体权力的关注，确保在安全合规的前提下，实现个人数据要素的流通共享。

4 保险行业个人信息保护执法案例与启示

在相关法律法规和监管规则的指导下，各相关监管机构开展对各自领域内的个人信息采集、使用、处理、加工等环节进行个人信息保护合规检查，并对相关违规行为进行通告处罚，从处罚结果情况来看，处罚体系具有全面性和严格性，既对个人也对组织进行惩罚，既有行政处罚也有金额处罚，需要引起保险机构高度重视。

国家金融监督管理总局与个人信息相关的行政处罚中出现频次较高的违法类型主要为：员工侵犯公民个人信息和利用职务泄露客户信息、未经授权或者超出授权范围收集、使用、保存、传输个人信息；未履行告知义务或者未取得同意；未采取必要的安全措施，导致个人信息泄露或者被非法获取；未按照规定报告网络安全事件；未按照规定配备网络安全管理人员和技术人员等。部分相关监管处罚情况请参加下表：

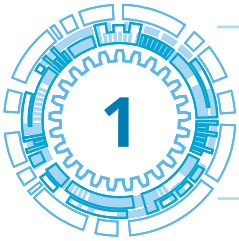
表1：部分相关监管处罚情况

监管机构	处罚时间	编号（文书/决字号等）	违法类型	（行政）处罚内容	作出处罚机构	被处罚机构/个人	处罚依据
国家金融监督管理总局	2023年7月7日	金罚决字〔2023〕1号	一是侵害消费者合法权益。包括：存在引人误解的金融营销宣传行为，侵害消费者知情权；未向部分客户群体明示还款要求；未按规定处理部分消费者个人信息。 二是违规参与银行保险机构业务活动。包括：违规参与保险代理、保险经纪业务；违规参与销售个人养老保障管理产品、银行理财产品、互联网存款产品。	没收违法所得112,977.62万元，罚款263,270.44万元，罚没合计376,248.06万元	国家金融监督管理总局	某集团	《中华人民共和国银行业监督管理法》第十九条、第四十四条，《中华人民共和国保险法》第六条、第一百一十九条、第一百五十九条，《中华人民共和国消费者权益保护法》第十四条、第十六条、第二十条、第二十六条、第二十九条、第五十六条等规定
原浙江银保监局	2023年3月6日	浙银保监罚决字〔2023〕3号	客户信息保护不审慎	对**银行罚款人民币30万元。	原浙江银保监局	某银行	《中华人民共和国银行业监督管理法》第四十六条第（五）项
原宁波银保监局	2023年1月18日	甬银保监罚决字〔2023〕10号	存在侵犯公民个人信息的违法违规行为	禁止终身从事银行业工作	原宁波银保监局	柴某	《中华人民共和国银行业监督管理法》第四十八条
原宁波银保监局	2023年1月18日	甬银保监罚决字〔2023〕8号	安防管理不到位、客户信息安全管理不到位	合计罚款人民币190万元	原宁波银保监局	某银行分行	《中华人民共和国银行业监督管理法》第四十六条
原六盘水银保监分局	2022年10月25日	六银保监罚决字〔2022〕13号	利用职务便利泄露在业务活动中知悉的投保人、被保险人个人信息行为的直接责任人	禁止进入保险业三年	原六盘水银保监分局	马某	《中华人民共和国保险法》第一百七十七条
原六盘水银保监分局	2022年10月25日	六银保监罚决字〔2022〕9号	案防管理不到位，原职工利用职务便利泄露在业务活动中知悉的投保人、被保险人的个人信息	罚款十万元	原六盘水银保监分局	某保险公司支公司	《中华人民共和国保险法》第一百六十一条
原六盘水银保监分局	2022年10月25日	六银保监罚决字〔2022〕12号	利用职务便利泄露在业务活动中知悉的投保人、被保险人个人信息行为的直接责任人	禁止进入保险业十年	原六盘水银保监分局	刘某	《中华人民共和国保险法》第一百七十七条
原六盘水银保监分局	2022年10月25日	六银保监罚决字〔2022〕10号	对**人寿保险股份有限公司六盘水中心支公司案防管理不到位，原职工利用职务便利泄露在业务活动中知悉的投保人、被保险人个人信息行为承担主要领导责任的直接责任人	警告并罚款二万元	原六盘水银保监分局	戴某	《中华人民共和国保险法》第一百七十一条
原宁夏银保监局	2022年8月18日	宁银保监罚决字〔2022〕19号	违反法律规定侵犯公民个人信息	对时任**保险股份有限公司宁夏分公司电网销业务部总经理徐**予以禁止进入保险业5年的行政处罚。	原宁夏银保监局	徐某	《中华人民共和国保险法》第一百七十七条
原宁夏银保监局	2022年8月17日	宁银保监罚决字〔2022〕18号	违反法律规定侵犯公民个人信息	对时任**保险股份有限公司宁夏分公司银川中心支公司创新电子部经理樊*、原**保险股份有限公司宁夏分公司员工刘*分别予以禁止进入保险业5年的行政处罚。	原宁夏银保监局	樊某、刘某	《中华人民共和国保险法》第一百七十七条

除此之外还有其他监管机构的处罚案例也值得引起行业关注，中国人民银行与个人信息相关的行政处罚中出现频次较高的违法类型主要为：未经授权查询个人信息；未建立以分级授权为核心的金融消费者信息使用管理制度，未准确披露因金融产品或者服务产生纠纷的处理及投诉途径；信息使用授权审批程序不规范；金融消费者投诉处理信息报送不及时。中华人民共和国工业和信息化部及中央网络安全和信息化委员会办公室与个人信息相关的行政处罚中出现频次较高的违法类型主要为：应用分发平台上的APP信息明示不到位；违规互联网弹窗信息推送服务；欺骗误导强迫用户；超范围收集个人信息；违规收集个人信息；APP强制、频繁、过度索取权限；收集个人信息明示、告知不到位；强迫收集非必要个人信息；违规使用第三方服务。

这些个人信息保护的处罚案例，无疑为整个保险行业敲响了警钟。这并不仅仅揭示了某些保险机构在个人信息处理中的失误和不当行为，更深层次的是，也反映了保险行业在个人信息保护方面普遍存在的问题和隐患。这些问题可能源于管理的不完善，也可能是技术上的疏漏，抑或是员工对个人信息保护意识的缺乏。但无论如何，这些问题的存在都使得客户的个人信息面临被泄露或滥用的风险，从而损害了客户的权益和信任，进而对保险机构的声誉造成损失，甚至是带来法律赔偿责任。

二、数字化转型背景下对保险行业个人信息保护能力建设的思考与应对



外规内化，健全个人信息治理体系

面对强监管环境、保险行业的复杂业态以及保险机构自身内部治理及协同机制不完善的情况，保险机构应积极主动采取对内、对外结合的应对措施提升个人信息保护管控水平，对机构内部需要建立明确的个人信息保护内部治理机制，并将监管要求进行内化，对监管、客户等外部需要统一对接归口，并建立透明的沟通机制。本节将从保险机构过往应对个人信息保护的经验出发，结合保险行业当前的实际情况，进一步阐述保险行业对个人信息保护的前瞻性应对策略。

落实个人信息治理部门责任，发挥组织推动和管理协调作用

个人信息与保险业务流程的深度融合决定了个人信息治理工作不是某个岗位、某个团队或某个部门能够单方面完成的工作。对保险机构而言，个人信息治理工作需要从组织战略层面出发，协调决策层、管理层和执行层等多方共同参与，构建个人信息治理合力，促成个人信息治理共识，消解个人信息治理壁垒，打通个人信息治理回路。

一是要明确个人信息主体治理架构，建立决策、管理、执行和监督机构，落实相关岗位和职责。在充分理解个人信息作为特殊的数据要素的前提下，由决策层决定安全合规发展方向，形成个人信息治理战略，促进个人信息保护文化，提供资源保障和决策支持；管理层拆解治理目标，推动各业务线、各部门、各团队及分支机构落地个人信息管理工作，发挥授权、指导和监督等职能，构建个人信息管理体系、设计个人信息管理流程、汇总和汇报个人信息管理现状等；各个人信息责任岗位及保险机构全体员工作为个人信息保护的执行层和第一线，理解机构个人信息治理目标，积极创新个人信息价值释放方式，严格执行个人信息保护各项要求，尊重客户个人信息权利；风险管理、内控和内审部门筑牢底线，充分监督个人信息治理工作的落实情况，为机构个人信息处理工作保驾护航，形成持续监控机制、及时预警机制和良性纠偏机制。上述工作对保险机构人员梯度建设提出了一定要求，其中个人信息保护相关法务专家、安全专家、业务专家及审计专家等角色设立是优先工作任务，能够帮助机构构建相对全面的治理和管理能力，充分理解组织情景，助力实现安全合规发展的个人信息治理目标。

此外，保险机构需要明确对外的统一接口部门，可分为面对监管机构和面对客户两个方面。首先，需要明确负责与监管机构对接的统一接口部门，负责进行信息报告、配合监管审查等流程，确保与监管机构的数据交流和信息披露符合法规要求。其次，明确面对客户的统一接口部门同样至关重要，保险机构需确保信息的安全传递、正确使用以及依法保护客户隐私，保险机构需要制定明确的工作流程，并定期进行培训，有效避免因信息处理不一致而带来的合规风险，提升机构整体的个人信息保护水平。

二是要建设跨部门协作机制，通过有效沟通平台，营造良好沟通氛围，促成个人信息治理共识的落地。在决策和管理层面，以个人信息治理管理委员会或个人信息专项工作小组形式，拉齐业务、科技、风险等部门认知，为跨部门协作奠定基础；通过定期或不定期会议、互动沟通等方式方法，形成部门间横向，部门内纵向的沟通协作平台，部署和落地个人信息治理工作具体事务。积极寻找跨条线、跨部门、跨团队利益交叉点，以安全合规发展为核心，多元主体共建内部个人信息治理环境，并通过跨部门个人信息治理绩效指标等工具树立共同的愿景和目标，以增强个人信息治理工作的内生动力。

完善个人信息治理制度，运用科技手段提升治理效能

保险机构的海量个人信息治理和管理工作需要依赖技术工具，同时还需要具备个人信息管理流程和风险数据应用能力。为快速形成全流程全领域个人信息治理管理能力，各机构可以考虑从以下三个点切入：

- **优化产品/服务创新引发的个人信息保护触发条件**：由于保险行业通过产品/服务创新进行数字化转型，这一过程伴随着众多基于新场景、新业务的新产品发布与使用，如核保核赔的智能回访服务。保险机构需以全程合规管控的视角将个人信息保护管控流程融入整个产品/服务创新的生命周期，确保创新过程在满足市场需求的同时，也充分遵循个人信息保护的法规要求。此外，保险机构需要根据业务运营的不同阶段和场景，制定灵活、差异化的个人信息保护触发条件，针对业务特点，动态选择适配的个人信息保护机制，确保在保单申请、理赔处理、个性化定价等各类保险业务场景下的个人信息保护措施能够全面、精准地发挥作用，满足保险业务的多元化需求。
- **采用先进技术驱动风险预测与响应**：借助人工智能、机器学习等先进技术，保险机构可对个人信息保护风险进行精准评估与监测，如在核保过程中，利用机器学习算法对客户的个人信息处理全生命周期进行分析，包括处理目的授权凭证分析、传输存储安全风险分析、数据超期处置分析等，自动判断潜在的隐私泄漏或滥用风险，并迅速采取相应措施。但需注意，在采用先进技术前，保险机构需要对技术的引入进行全面的风险评估，减轻新技术带来的隐私风险。
- **引入协同工具与平台，建立信息共享与集成机制**：保险机构应使用满足公司规模和需求的协同工具或平台，通过在工具或平台上设立专门的工作空间，存储与个人信息保护相关的制度、指南等文档，并为各部门之间的信息流通提供安全通道，在遵守监管要求的基础上实现跨部门的信息共享与集成，避免客户个人信息冗余收集和处理，同时确保业务、科技与合规等部门的工作更加紧密、高效地协同进行。在使用协同工具与平台时，注意需要通过采用授权审批、日志记录等安全功能提高信息流动的透明度与安全性。

优化个人信息合规性管理，主动构建安全高效的金融服务生态

数字化转型背景下，开放平台的技术架构正不断重塑金融服务价值链；保险机构深度参与其中，并通过个人信息创新服务场景，丰富保险产品和营销渠道。这一时代背景和市场动向催生了保险机构主动构建安全高效的金融服务生态。

为积极承担和履行市场主体责任，保险机构可以考虑从以下三个方面入手，依法依规开展业务、积极创新合作共赢，有效协调和管理价值链中涉及个人信息处理的关键主体和关键活动。

- **回归本源严守底线**，以人为本统筹机构安全和发展，积极参与政策制定过程和行业主管部门组织的各项活动，定期与监管部门进行深度沟通等，提供个人信息保护的相关建议。从金融伦理等角度出发，合理有序发出机构声音，促进符合行业发展需要、技术动态和风险控制能力的政策环境。
- **建立透明的客户沟通机制**：保险机构应该通过面向客户的统一接口部门与客户积极建立有效且透明的沟通机制，明确向客户详细解释保险机构的隐私政策，包括数据收集目的、使用方式、安全措施、隐私政策变更等内容。通过与客户的透明沟通，积极引导客户主动地参与到个人信息保护工作中，并增强客户对机构的信任度。
- **践行社会责任与行业合作**：保险机构应积极履行社会责任，通过参与行业合作，通过与行业相关协会开展相关话题的研讨与沟通，促进行业标准的制定和升级，推动整个保险行业在个人信息保护方面的共同进步。保险机构也可通过参与上下游业务、技术相关方组织的活动，分享个人信息保护的最佳实践、经验和技术，助力更加完善的行业生态形成。

建章立制，体系化增强个人信息管理能力

通过体系化建设个人信息保护管理能力，全面防范保险业个人信息安全风险。本节将从个人信息收集和使用的角度出发，重点关注个人信息分类分级管理、个人信息安全影响评估、个人信息处理第三方管理、个人信息跨境安全的能力建设，由点及面，筑建个人信息保护城墙。

完善分类分级管理制度，明确个人信息保护策略

建章立制，完善个人信息分类分级管理制度，实施差异化保护。保险业处理大量健康医疗数据、个人金融信息等敏感个人信息，结合数据分类分级体系框架，细化个人信息分类分级管理要求，落实个人信息生命周期、处理活动各环节差异化管控措施，有效防范个人信息安全事件。

个人信息分类分级管理制度的建立，**一是要明确适用的个人信息分类分级标准**。结合梳理、掌握的个人信息资产情况，参照监管要求和行业标准，定义不同个人信息类别，如个人基本信息、个人健康生理信息、个人财产信息等；根据实际业务场景分析可能的个人信息泄露影响程度、个人信息敏感程度和行业标准，定义个人信息级别，如内部使用、保密、高度保密或C1（用户鉴别信息等）、C2（可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息）、C3（机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息）等。**二是要结合个人信息生命周期细化差异化的管理要求**。对于个人信息的收集、传输、存储、使用删除及销毁等环节的处理活动，根据个人信息分类分级不同提出差异化的管理要求，如收集个人信息获取同意环节，针对一般个人信息获取授权同意即可满足管理要求，但针对敏感个人信息、个人生物识别信息需要获得明示同意，而针对不满14周岁未成年应征得其监护人明示同意。**三是推动分类分级管理要求落地和持续改进**。在落实相关差异化管理要求过程中，需多方协同，如由业务部门对处理的个人信息类别和级别进行识别，由科技部门通过部署技术手段和工具满足保护要求；而且个人信息分类分级管理受业务发展、法律法规变化、技术进步等趋势影响，应保持动态管理的状态，通过持续的监测、定期的风险评估和审计，判断数据分类分级管理的有效性，根据实际情况进行改进和优化。

落地个人信息安全影响评估（PIA），护航创新业务发展

《中华人民共和国个人信息保护法》中明确了开展个人信息安全影响评估的条件和内容；开展相关评估有利于识别企业内个人信息处理活动、确定个人信息获取同意方式、评估个人信息处理合规风险，预防踩红线情况发生。

个人信息安全影响评估机制的建立，**一是要明确评估流程和责任方，设计有效评估工具。**确定个人信息安全影响评估的类型和适用场景，固化评估实施步骤和环节（如数据映射分析、评估问卷填写、安全影响评估分析、评估结果跟进等），明确个人信息保护主管部门、业务部门、科技部门、法务合规部门在各环节的主要角色和职责，设计适用的评估工具，综合参考《中华人民共和国个人信息保护法》《信息安全技术个人信息安全规范》《信息安全技术个人信息安全影响评估指南》《个人金融信息保护技术规范》等要求，设计包含不同筛选条件和赋值的自动化工具，从产品技术架构中的消息中间件、API、数据库等关键传输链路和关键存储节点收集数据信息，主动探知安全风险，例如传输存储未加密的数据泄露风险、批量数据查询和数据导出的滥用风险等。**二是要加强业务团队数据能力建设，推动业务部门主动触发所辖个人信息处理活动影响评估。**对于个人信息映射规则、标准、评估工具使用方法开展培训，统一认知，便于后续顺利进行；由个人信息保护主管部门组织业务部门开展个人信息安全影响评估，由科技部门、法务合规部门协同确认相关技术实践和法规解读，分场景识别个人信息处理活动中依赖的基本要素和流转关系（如个人信息处理环节、依赖的系统资源、相关方识别、个人信息流转分布情况等），全面分析对个人信息安全造成影响的因素和风险。**三是建立个人信息处理活动台账，对风险问题完成整改追踪。**结合个人信息安全影响评估结果，梳理个人信息处理活动，形成个人信息资产清单；分析个人信息处理环节的合法、正当、必要性，确保满足个人信息处理活动的基本原则；识别个人信息保护全生命周期管控要求和差距，如个人信息处理活动告知及获取同意的要求、方式，系统及安全控制的技术改进意见，相关保险业务环节及工作流程的变化要求等；由相关部门针对评估结果提出整改方案和整改计划，由个人信息保护主管部门跟踪整改情况和结果。

加强第三方数据合作安全评估，坚持个人信息管理责任不外包

共筑个人信息保护长城，加强个人信息处理第三方管理，明确职责划分。保险业经常面临多险企及第三方机构共同处理客户个人信息的场景，如未在合作过程中明确双方或多方主体性质、权利义务、违规责任承担等内容，一旦发生个人信息安全事件，双方或多方之间的责任划分、赔偿分摊比例等问题将引发更多次生风险。

在对个人信息处理第三方管理的过程中，可以依托企业已有的第三方管理体系和流程，结合个人信息安全保护要求加强管理，如在**第三方筛选评估阶段**，对第三方进行审查和评估时应增加关于第三方个人信息保护体系建设或业务处理中的个人信息保护要求的建设情况、个人信息的相关安全设施和技术能力、个人信息安全事件响应流程、个人数据主体的请求及投诉处理机制的评估内容。在**与第三方签订服务合同阶段**，应明确第三方处理活动的性质（间接收集、委托处理、共享转让）、客户个人信息的处理方式、使用范围、信息安全保障和违规时的内容等。在**签订服务合同后**，定期向个人信息保护主管部门报告，更新委托业务清单、隐私政策等；定期对第三方的个人信息保护措施落实情况进行安全评估、现场检查等。在**服务结束或终止后**，应监督第三方销毁因相关业务或服务获取的个人信息。

在个人信息处理中还有一类第三方合作模式，即第三方产品或服务嵌入企业自身产品或服务的情况。一方面需要通过合同形式明确双方安全责任，且向个人信息主体明确标识该产品或服务由第三方提供。另一方面需要由科技部门对外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）开展安全测试，确保其个人信息收集、使用行为符合约定要求。

选择个人信息出境路由，释放跨境业务红利

立足中国，放眼全球，保护个人信息跨境安全，维护国家网络安全。随着中国市场的国际化，一方面中外合资或外商独资保险机构面临个人信息出境处理，另一方面中国企业出海、全球布局也面临个人信息跨境合规挑战。

个人信息跨境安全评估，**首先需要识别当地的个人信息出境要求和豁免条件，选择恰当的合规路径。**对于出海企业，需要了解当地特殊的个人信息出境限制和豁免条件，如欧盟《通用数据保护条例》（GDPR）、亚太经合组织倡导的CBPR、全球发展倡议框架等。

对于中国大陆个人信息出境，保险机构需要在遵循合理合法必要的前提下，充分考虑出境场景、数据数量，选取与机构发展运营模式、技术能力和风险态势相适应的出境路由，包括安全评估路由、个人信息保护认证途径和标准合同模式。评估个人信息出境的必要性和合法合规性，记录个人信息出境详情，约定发送、接受各方权责义务。**其次需要评估数据出境安全风险。**数据出境安全风险评估主要评估个人信息出境和境外处理的目的、范围、方式的合法、正当、必要性，出境个人信息的规模、范围、种类、敏感程度对国家安全、公共利益、个人或组织合法权益带来的风险，境外接收方承诺承担的责任义务以及履行该责任义务的管理和技术措施、能力等能否保障出境数据的安全，个人信息权益维护的渠道是否通畅等影响数据出境安全的事项。例如出境个人信息被接收方滥用的风险、出境个人信息泄露机构市场策略影响机构正常经营或声誉风险，甚至出境个人信息涉及金融敏感信息危害国家安全的风险。出境安全风险评估是充分理解并落实跨境业务安全合规发展的必由之路，保险机构可借此在复杂多变的地缘政治背景下守正创新，良性利用两个市场发展机会。**最后需要完成相应监管申报动作，并保持对监管动态的追踪和出境申报材料的更新。**不同的合规路径选择需要准备的申报材料不同，如中国个人信息出境安全评估申报和标准合同备案所需的评估内容和准备材料存在差异，需花费的努力也不同，企业应在个人信息出境前完成相关评估、整改和申报工作，因此需要对于整体项目、业务或系统推进的周期提前做好规划。在完成相应监管申报后，企业还应持续关注本地监管环境变化、个人信息出境实践趋势，及时做好应对；另外还应持续关注出境的个人信息处理活动变化，一旦向境外提供个人信息的目的、方式、范围、种类、保存期限或境外监管和网络安全环境发生变化，需要再次评估个人信息出境风险。

3 技术破局，强化个人信息安全合规利用

通过体系化建设个人信息保护技术能力，实现对个人信息全生命周期的安全性与完整性，同时也能有效保护个人隐私，确保数据处理与利用符合各种法规与合规性要求。本节将对隐私增强技术、代理重加密、移动应用合规检测等技术如何应用到个人信息安全合规保护场景进行探讨，以协助各保险机构对个人信息技术体系建设。

选用恰当的隐私增强技术，应对不同场景的数据安全需求

从共享数据源来看，保险机构通过三种方式共享个人信息以实现潜在的数据价值，包括入站数据共享（从第三方获取数据）、出站数据共享（与第三方共享自有数据）和协作数据共享。

入站数据共享强有力地支持了保险机构的经营，例如保险营销数据的获取；另一方面，出站数据共享实现多角度赋能，例如线上线下融合营销等；最后，协作数据共享挖掘了行业数据价值，使得保险机构能够获得更深和更广的洞察，典型的场景莫过于“了解你的客户（KYC）”。

共享数据的意义不仅在于为保险机构创造利润，也在于为保险客户提供更精准更高效的产品和服务，并使客户日益认识到其个人信息的价值。在主管和监管部门指导和监督下，安全合规的数据共享，将壮大保险市场各参与主体的力量，造就更好的金融成果。

当前数据共享客观存在一系列挑战，包括数据滥用风险、监管合规风险、共享数据管理成本甚至是客户的信任危机。

图1：数据应用的价值与挑战

共享数据的潜在价值		共享数据的潜在威胁
支持经营决策	保险机构	泄露业务竞争策略
引入第三方能力		违反个保法律法规
获取更多的数据		引起客户信任危机
促进创新和竞争	监管部门	侵犯客户个人信息权益
提供有效的监督		
获取优质产品服务	客户	滥用个人数据
获取精准产品服务		泄露敏感信息

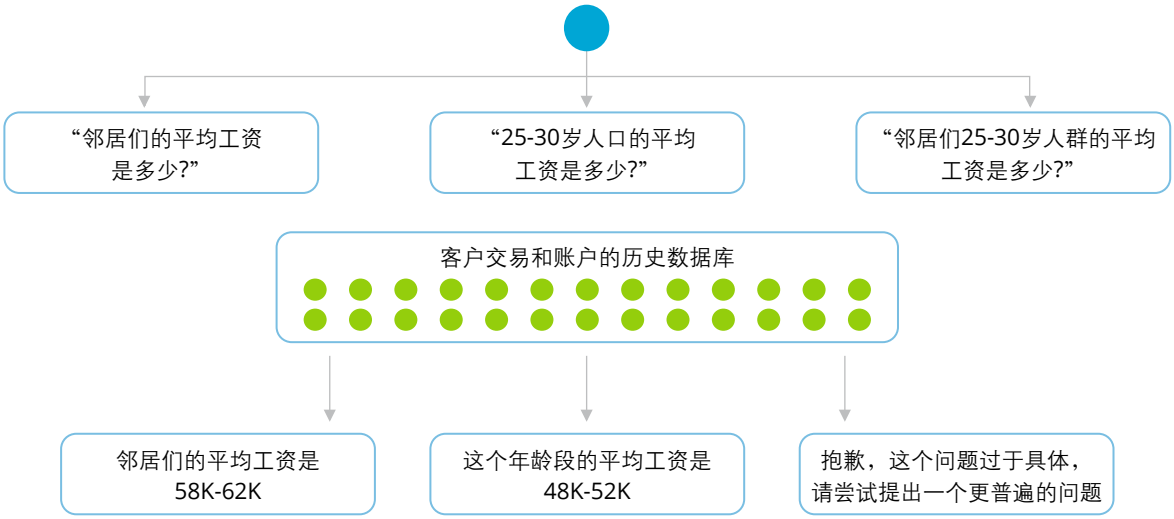
如图所示，保险行业的各个参与主体在个人信息保护领域面临着不可忽视的矛盾。然而，新兴的隐私增强技术使得平衡保险机构、客户和监管部门在数据共享场景下的诉求和义务成为可能；使数据共享符合监管原则，保护客户隐私，并保障保险机构业务的保密性；并将扩大保险行业可行的数据共享的范围，有效地让保险机构深入行业数据，释放出新的价值。安全合规的数据共享，为保险机构、客户、监管部门和整个社会构建更广阔的发展空间。

差分隐私、联邦学习、同态加密、零知识证明和安全多方计算等隐私增强技术在近几年得到长足发展并逐步展现其价值。

差分隐私

当保险机构寻求与第三方共享数据时，删除或匿名化个人身份信息并不总能保护数据库中个人的隐私。例如，数据可以与其他数据集相关联，从而重新识别数据库中的特定个人。解决这个问题的一个行之有效的方法是在处理过程中添加噪音（输入、计算或输出），从而确保一条记录的隐私，同时获得有意义的信息。差分隐私致力于解决这方面的问题，使得共享数据的接受方无法通过特定条件筛选出可能存在隐私泄露风险的记录。例如在智能营销顾问场景中，机构基于用户同意共享部分数据，而在数据集相对小的情况下，营销渠道可能具备重新识别客户个人信息的能力；而客户则可能对不加限制的共享产生厌恶。差分隐私可用于在类似的共享和分析过程中引入噪音，确保数据集中的个人隐私不受侵犯并提供充分的洞察。

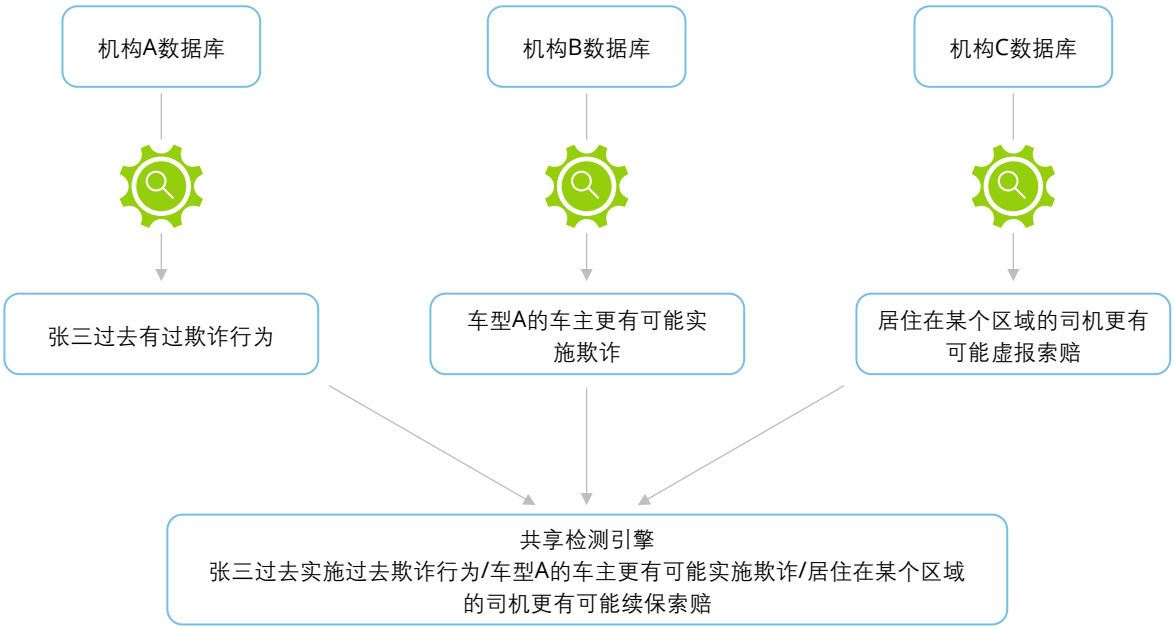
图2：差分隐私场景应用



联邦学习

当保险机构需要分析大量数据集，尤其是涉及集团下多个经营主体的数据集，合并这些数据到一个数据库开展工作往往并不可行。主要的风险考量包括：个人信息的本地化存储限制、个人信息主体授权限制、数据集中泄漏风险等。联邦学习可以作为该场景下的解决方案，即对不同的数据集分别进行分析，然后在各数据集之间共享分析结果。例如在反欺诈工作中，保险机构如果能够共享客户登记信息、投保资产、理赔信息甚至是医疗报告，将为机构识别欺诈模式、规避重复理赔等损失风险提供极大帮助。联邦学习可以通过在不跨机构共享数据的前提下，构建主欺诈检测模型，覆盖投保至理赔全周期；保护客户个人敏感信息，并确保保险机构不会因数据共享而泄露承保和定价策略等商业机密。

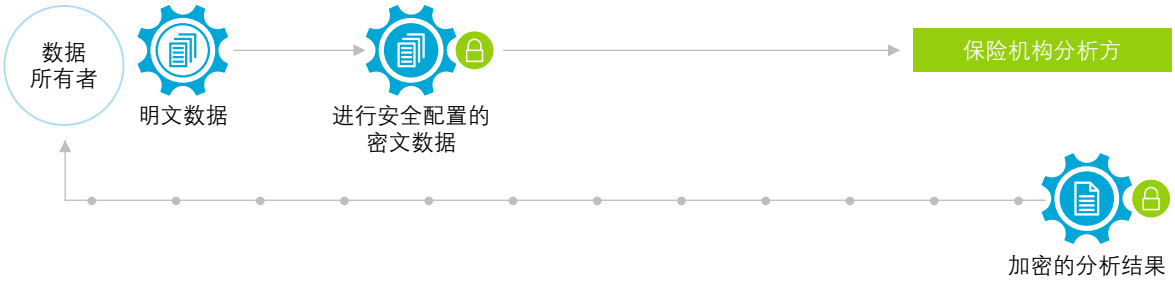
图3：联邦学习场景应用



同态加密

当保险机构希望委托第三方处理个人信息，或允许第三方补充数据集以增强分析能力时，常面临与前文类似的风险，包括数据共享或传输范围失控、信任关系受损以及数据泄露或滥用风险等。同态加密可用于应对这些挑战，它可以对已加密的数据进行分析，与此同时，信息本身不会被分析方解密；分析结果也不会被授权方（通常是个人信息处理者）以外的任何人读取。在包括存储、计算等场景在内的“一切皆服务（XaaS）”的今天，同态加密在委托数据处理、模型训练和反欺诈等方面的价值不言自明；然而其相对缓慢的处理速度及全密态分析过程带来的对分析结果可信度的疑虑，使这一技术的推广应用伴随着诸多挑战。

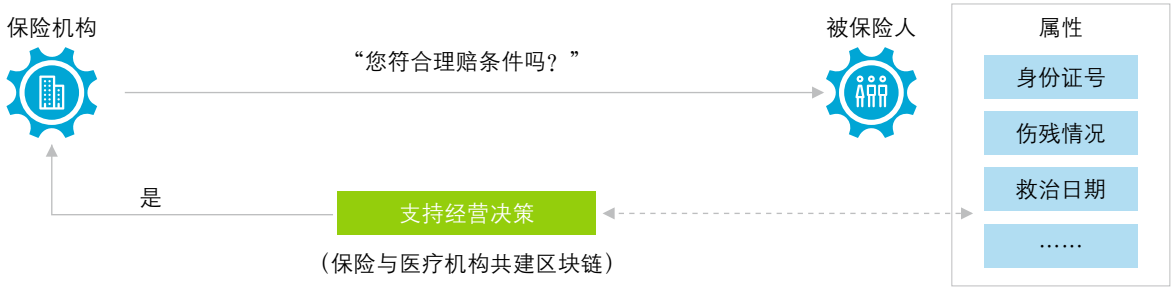
图4：同态加密场景应用



零知识证明

保险机构能够通过更精准的信息为客户提供更高效的服务，并创造更大的利润。然而客户与机构的博弈是客观存在的：客户通过包装自己的资产情况、健康情况，以期在投保环节获得更低的折扣，这种情况并不鲜见。传统上，机构可能会以客户的健康档案或其他资信证明为准，然而这类凭证的伪造案例层出不穷。零知识证明（ZKP）能够有力地解决这一问题，近几年随着区块链技术的长足进步，零知识证明的应用愈加广泛，尤其在KYC方面，帮助试水的保险机构以最少的个人信息、最低的隐私风险证明了客户的各项属性。例如被保险人因意外伤害导致身体全残需索赔，机构为帮助客户快速取得相应权益以慰人心，可以通过与医疗机构共建的ZKP系统实现传统理赔流程不可企及的效率。

图5：零知识证明场景应用



安全多方计算

与同态加密和零知识证明一样，安全多方计算（SMC）技术允许在与不受信任的第三方共享信息的同时维护个人信息安全。传统来说，多方共享数据往往需要一个可信中介，而这一实体的引入带来了新的数据泄露和滥用风险，同时，也不能完全规避数据共享场景下的数据安全责任。安全多方计算技术将中间人替换为安全的算法，即使部分数据被截取，也不会暴露任何敏感信息。SMC依靠的是“秘密共享”，即把每个贡献者的敏感数据以加密“共享”的形式分配给每个参与方。例如，在保险机构与医疗机构联合处理医疗健康数据以实现理赔、结算等服务时，各参与方基于数据安全配置进入多方计算环境，调用分析平台规则，实现服务价值增长、数据不出域、风险不增加的数据利用目标。

图6：安全多方计算场景应用

分析结论：某地区各年龄段死亡率显著低于平均值，考虑降低保费以提升竞争力

代理重加密破解数据共享谜题

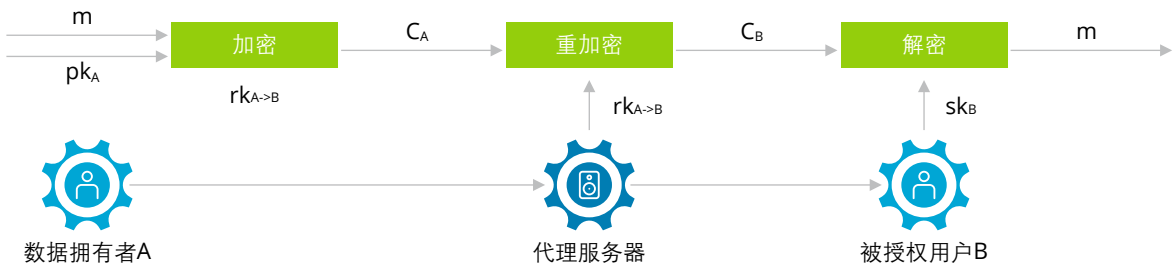
部分保险机构作为集团旗下专业公司积极发展，自身积累了大量的客户数据可供合规输出，同时也对利用集团数据充满期望。在保险行业数字化转型的大背景下，集团间各专业公司实现数据共享将释放更多的价值红利。然而，安全合规共享数据的挑战不可忽视，开启数据共享大门，种种问题纷至沓来。各专业公司作为数据所有者如何授权其他专业公司使用数据？如何控制共享数据的使用范围、时间和目的？多主体对多主体的各数据集授权与被授权复杂网络如何实现？数据共享中的传输和存储安全如何保证？

诸如此类的问题横亘在保险机构面前，而代理重加密技术另辟蹊径，开拓了集团内数据共享的途径。

代理重加密是一种具有密文安全转换功能的新型公钥加密体制，数据所有者和被授权者是共享数据的通信双方，通常由数据拥有者来生成解密权指派所需的代理重加密密钥；而代理服务器将负责执行重加密和实际的授权动作。代理重加密区别于传统加密体制的最大特点在于数据所有者和共享数据的接收方并不直接通信，而是由数据所有者使用自身公钥将数据加密后存储于代理服务器，数据接收方自代理服务器获得可由其私钥解密的密文。显然，在数据接受方获取数据前，代理服务器完成了密文的转换，这一转换依赖于由数据拥有者提供的代理重加密密钥；当且仅当这一密钥使用数据接收者的公钥生成时，接收方能够解密代理服务器中的密文。

上述动作实际完成了数据拥有者对数据接收方的数据共享授权，同时，传输链路及代理服务器中的静态数据保持全流程密文，也降低了数据共享过程中明文传输、存储的风险。配合集团设立、与专业公司隔离的专有数据安全域，集中管控数据销毁周期和基础设施，能够有效解决多主体间数据共享追溯、审计、使用目的和共享期限问题，大大提高了集团内多主体数据共享的安全性和合规性。

图7：代理重加密概念架构



移动应用合规检测技术，筑牢渠道安全底线

移动互联网应用（App）已经成为保险机构无可争议的重要经营渠道，其具备不可替代的持续采集和灵活运用个人信息的能力，以及全天候随时触达客户的可能性。然而，随着监管加速，移动应用违法违规收集使用个人信息的判断条件不断细化、处罚日益严格，App动辄面临警告，甚至下架的风险。此外，App自身的快速迭代以及第三方SDK的使用，都使得相关合规工作成为一场持久战。

移动应用的持续化自动化合规监测技术成为破题的关键。App安全合规检测通过分析App中的隐私政策、权限申请、数据收集和使用等方面是否符合法律要求和安全标准，实现对个人信息风险研判和保护。通过对检出风险的持续改进，为用户的隐私权益提供持续的保护，保障业务平稳运行。

App安全合规监测技术包括静态代码分析和动态沙箱监测，以及插桩技术和网络流量捕获等方法。静态代码分析可以在代码级别发现潜在的安全问题，而动态沙箱检测则可以在运行时检测App的行为。插桩技术和网络流量捕获则可以深入到App的内部，检测其对系统资源的使用和网络通信行为。此外，保险机构还可以在开发阶段等各阶段插入自定义安全检测逻辑，实现深入彻底的安全合规自查。这种方法可以在开发过程中及时发现和修复安全问题，大大提高了App的安全性。

图8：APP隐私合规检测要点

1

App收集使用个人信息合规评估
依据《App违法违规收集使用个人信息行为认定方法》等文件，针对App进行评估，发现可能存在的收集使用个人信息方面的问题。

2

隐私条款评估
依据《个人信息安全规范》及隐私条款专项工作评审要点等文件，针对App的隐私条款进行评估，发现隐私条款及相关实现机制存在的不足。

3

第三方SDK分析
发现第三方SDK集成情况，并对相关SDK调用权限进行定位，了解和评估第三方SDK行为，为SDK超采治理提供支持。

4

权限检测
通过静态分析识别App声明调用系统权限情况，并结合动态模拟，判断是否存在过度索权行为。

5

隐私设计检测（PbD）
针对隐私政策明示、权限用途明示、账户注销、隐私设置、个性化推送、隐私政策入口等合规关注的隐私设计要点进行评估并存证。

6

应用行为轨迹信息
结合时下C端用户关注热点，模拟一段时间内App行为，记录应用行为轨迹，用于评估实际使用场景下，后台权限调用及个人信息使用情况。

除移动客户端安全外，服务端安全也是保险机构需要重点关注的问题；后者一旦失陷，可能造成严重的个人信息安全事件。而在保险机构多渠道展业的背景下，又以服务端应用程序接口（API）安全为甚，近几年由于相关问题导致的安全事件屡见不鲜，其泄露的个人信息记录条数以亿计；API安全问题带来个人信息风险包括未授权访问、泄露和滥用等。API的广泛使用使得保险机构系统暴露了前所未有的攻击面；而结合自动探测和历史资产导入的数字化资产管理方案，配合常态化的攻防验证为保险机构安全运营提供了新的破题思路。

4 动态持续追踪，增强运营韧性

保险机构在个人信息安全运营中同时面临着外部和内部的压力；外部压力包括个人信息主体权利响应、个人信息事件等。内部压力包括个人信息共享红线把控、个人信息安全共享要求满足等统筹安全和发展的压力。本节将从个人信息主体权利响应、共享安全风险应对、安全运营机制等角度提出应对策略。

以人为本，理顺个人信息主体权利响应机制

保险机构作为个人信息的处理者，基于个人信息拓展业务获取合理的经营利润，有义务响应和满足个人信息主体权利满足，包括完善个人信息主体权利满足监控与评估机制、建立便捷的个人信息主体权利响应机制，并关注近年来争议较多的自动化决策下个人信息主体权利的满足。

一是完善个人信息主体权利满足监控与评估机制，梳理法律法规及监管要求中各项个人信息主体权利要求，定期根据合规要求中规定的需满足的个人信息主体权利项，开展集团下各金融产品的合规满足评估，并根据评估结果及时整改，做到“主动式”个人信息主体权利满足。

二是建立便捷的个人信息主体权利响应机制，为客户提供多样的权利满足渠道，包括个人信息主体权利实现在线申请平台、客服热线投诉电话、个人信息自助查询平台等。在核保、理赔和退保等全流程服务考虑将个人信息主体的权利保障机制内嵌在各个服务环节中，例如，建议保险机构在全流程中为客户提供自助查询服务，以保障用户的查阅权；在退保环节，可以考虑设置在线服务平台以供客户进行个人信息删除申请，响应个人信息主体的删除权。此外，建议保险机构简化个人信息主体权利满足申请流程，例如，简化客服热线转接投诉步骤，保障消费者拨打客服热线时最多转拨2次即可进入人工投诉通道。

三是关注自动化决策下个人信息主体权利的满足。保险机构可能会在保险核保、保险理赔和精准营销等场景中使用自动化决策。对于精准营销场景，通过自动化决策的方式进行精准营销，需要同时向个人提供便捷的拒绝方式。对于报销核保和保险理赔等场景，利用个人信息进行自动化决策时，应保证决策的透明度和结果公平、公正，不得对个人信息主体在交易条件上实行不合理的差别待遇。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。

明确共享管理机制，有序推动数据安全共享

保险机构作为金融服务开放价值链的一环，充分利用链上资源的同时，也在通过数据共享塑造合作共赢的金融服务生态。然而，价值释放与安全风险是个人信息共享的一体两面。保险机构需要重视共享安全，通过提高集团间个人信息共享安全意识、把控个人信息共享红线、明确个人信息共享的权利与义务，和遵守个人信息共享中的安全要求，打好安全基础，为个人信息价值发挥保驾护航。

一是建立与集团各专业公司发展需求、技术实力和风险管控能力相适应的共享模式。目前尚未存在相关法律法规和标准规范对集团内部的个人信息共享进行豁免，也没有放宽个人信息共享双方需履行的义务。集团内不同实体之间的个人信息共享仍需要遵循相关法规要求的个人信息使用目的的限制，并确保采取了相应的安全管理和技术措施。

二是把控个人信息共享红线。在实施个人信息共享前，对共享的个人信息类型进行判断，判断是否为限制共享的个人信息类型。目前，部分合规要求中，已明确限制共享的个人信息类型，例如根据金融行业标准，个人健康生理信息为4级数据，而金融机构不应共享4级数据，不应对4级数据进行委托处理。因此，保险机构在进行个人信息流动共享时，不应共享或委托处理个人健康生理信息。

三是明确个人信息共享的权利与义务。个人信息共享类型包括共享、委托处理和转移等。不同的个人信息共享类型，影响个人信息发送机构和个人信息接收机构的权利与义务履行。共享类型是指个人信息共享后，双方均拥有独立控制权；委托处理类型中受托人对该个人信息没有独立控制权；转移类型是指个人信息控制权由一个控制者转移向另一个控制者。各共享类型就各方是否拥有控制权存在差异，影响着安全管理义务的履行，例如共享类型的个人信息接收方由于拥有个人信息的独立控制权，允许其在获得个人信息主体单独同意的前提下变更原先约定的个人信息处理目的、处理方式和处理个人信息种类等。

四是遵守个人信息共享中的安全要求。机构应关注个人信息共享前、个人信息共享过程中、个人信息共享后的安全要求。个人信息共享前，个人信息共享双方应通过合同协议等方式，书面明确双方在个人信息安全方面的责任和义务，并约定个人信息共享的内容、用途和使用范围等，告知个人信息主体共享个人信息的目的、个人信息接收方的类型以及可能产生的后果等信息。此外，个人信息发送机构应针对个人信息接收机构进行个人信息安全影响评估等，以确保个人信息接收方采取有效的安全保护措施。个人信息共享过程中，应对个人信息共享过程进行记录，并采取个人信息安全保护措施，例如利用自动化工具如代码、脚本、接口软件开发工具包等进行个人信息共享时，个人信息共享双方应通过身份认证、数据加密、反爬虫机制、攻击防护和流量监控等手段，有效防范网络监听、接口滥用等网络攻击。个人信息共享后，应定期检查个人信息接收方的安全保护情况，并在个人信息主体提出个人信息主体权利相应要求时，与个人信息接收方共同响应个人信息主体权利。

构建安全运营机制，持续提高个人信息风险检测、预警和应急能力

随着人们对个人隐私的关注越来越高，个人信息安全事件处置不当对于保险机构的声誉将带来重创。个人信息安全事件的及时处置需要未雨绸缪，夯实机制基础、加强预警监测能力并开展应急演练，激发事件解决动能。

一是夯实机制基础。建议保险机构建立个人信息安全事件机制，设立由应急领导小组、应急指挥小组、应急执行小组、应急保障小组、应急报告协调小组组成的个人信息安全事件应急组织架构；按照安全事件的影响范围及持续时间等维度，划定个人信息安全事件等级，就不同事件等级明确事件响应步骤；明确个人信息安全事件应急流程包括监测预警、应急准备、应急处置、总结报告和应急解除等环节。

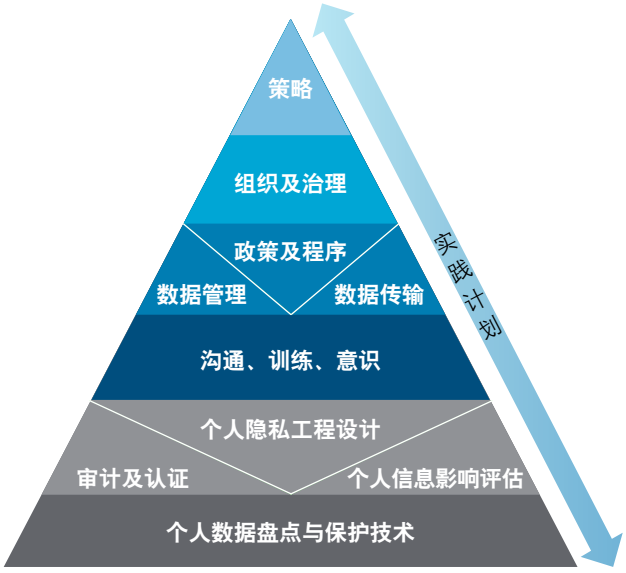
二是加强预警监测能力。密切关注业务日常运营中所出现的可能反映异常的特征，例如：敏感操作、流量异常、设备故障等，以此判断是否存在个人信息异常情况。根据需要监控的重要业务，识别可能出现个人信息安全事件的关键时点，例如：系统变更、部署新系统策略或账号权限变更、个人信息导出等。针对这些已经识别出来的关键时点，指定专门人员密切关注、持续跟踪关键时点业务的持续运营状况或资源的使用情况。此外，通过密切关注各大主流媒体，安全论坛网络舆情，查看是否存在保险机构的负面信息。

三是开展应急演练。建议保险机构制定个人信息安全事件相关应急演练计划，覆盖多场景的安全事件，例如办公终端个人信息外泄、数据库个人信息外泄等，协调相关部门与人员参加，提升个人信息事件紧急处置能力。应急演练完毕后，建议对应急演练过程进行复盘，发现应急预案以及应急演练过程中的不足，不断调整和完善应急预案和应急演练过程。

5 盱衡全局，制定特定的推进策略

综上所述，本报告针对保险机构的个人信息保护，从个人信息保护治理、建章立制、技术破局、管控运营等角度进行了探讨和分析。然而在保险机构在制定个人信息保护应对策略时，还需要充分结合内外部环境因素，开展定制化的推进策略，包括法律法规、行业规定、技术发展以及公司自身的业务需求和风险状况。为了方便保险机构从全局视角统筹开展个人信息保护策略的制定，本节将对个人信息保护总体策略给出构建模型，以方便保险机构结合特定需求和情况开展推进策略。

图9：个人信息保护模型



第一层　策略
- 确认保险机构高阶方向及风险偏好

第二层　组织与治理
- 建立有效的个人信息保护治理与管理框架

第三层　政策与流程
- 丰富保险机构管理、协同的制度、策略和文件

第四层　沟通、训练、意识
- 建立保险机构的个人信息保护意识

第五层　动态的控制措施
- 通过动态个人信息影响评估来识别应对风险

第六层　数据盘点及安全技术控制措施
- 盘点数据，健全安全技术防护措施

在策略方面，保险机构在应对个人信息保护时，首先应明确组织的战略方向和风险偏好，并在此基础上建立个人信息保护总体策略，过程中需要考虑保险机构自身的业务原则，确保个人信息保护策略与业务发展方向保持一致。

在组织与治理方面，应明确个人信息保护的治理模式、管理组织架构，过程中需要结合保险机构自身的发展规划、企业规模及其他关键利益相关者情况，并根据法规和监管等要求明确个人信息保护角色和职责。

在政策与流程方面，按照总体个人信息保护策略，明确个人信息保护的具体制度、策略及相关隐私政策等管理和技术要求，过程中需要结合治理模式、组织架构设计以及不同业态对个人信息采集、使用和处理的场景需求。

在沟通与意识方面，通过定期举办个人信息保护相关活动实现，如个人信息保护培训、个人信息保护日、个人信息宣传材料投放等形式，过程中要注意的是应根据不同级别、不同岗位的员工进行差异化调整。

在动态的控制措施方面，需要评估现行的个人信息保护机制以及相关项目管理方法，完善动态的控制措施，过程中特别需要注意的是在有新系统或重大变更时，应重新进行个人信息保护评估，评估的最终目的是识别潜在风险并提前应对。

在数据盘点与安全控制措施层面，应识别个人信息资产清单并明确个人信息的流转情况，结合个人信息资产清单的分布和流转情况，通过专业技术应用，强化个人信息保护能力。

在数字化转型时代，如何建立与本机构相适应的个人信息治理、管理和技术框架，实现安全合规发展的目标是各保险机构的重要议题。这一目标的实现需要各机构充分理解自身禀赋，包括存量数据资源、技术架构支撑、科技管理模式、数据应用能力等，结合市场需求、业务发展需要、技术能力和风险管控能力，制定个人信息治理战略，层层分解，明确实施路径和发展路线图，明确优先任务，在安全合规的前提下，充分释放个人信息特殊数据要素的价值。

结语

在数字化转型时代，随着保险业务线上化、数字化、智能化的日益普遍，个人信息保护已成为保险行业的核心议题。考虑到不同机构在企业规模、业务模式、数字化成熟度等方面的差异，在个人信息保护方面面临的具体难点挑战和应对策略也会不同，德勤保险行业团队会持续关注保险行业个人信息保护领域的相关话题，我们期望通过本报告能够引发保险机构更多的探讨与沟通。

最后，真挚地期望能够通过本报告给保险机构提供参考、引起共鸣，以期待构建全方位、多层次的个人信息保护机制，为个人信息保护筑起一道坚固的安全屏障，为保险机构自身基业长青、持续发展奠定坚实基础，推动保险行业健康、稳定地发展。

作者

何晓明
德勤中国网络安全服务合伙人
电话：+86 10 8512 5312
电子邮件：the@deloitte.com.cn

薛厂厂
德勤中国网络安全服务副总监
电话：+86 531 8165 1283
电子邮件：cxue@deloitte.com.cn

致谢

特别感谢德勤中国刘贤康、杨斐嘉、欧阳乐源、王雅超等多位同事对本报告撰写及发布所作的贡献。

特别感谢《中国银行保险报》发起本次课题研究、筹办课题研讨会及在课题研究过程中给予的大力支持与帮助。

办事处地址

北京
北京市朝阳区针织路23号楼
国寿金融中心12层
邮政编码：100026
电话：+86 10 8520 7788
传真：+86 10 6508 8781

长沙
长沙市开福区芙蓉北路一段109号
华创国际广场3号栋20楼
邮政编码：410008
电话：+86 731 8522 8790
传真：+86 731 8522 8230

成都
成都市高新区交子大道365号
中海国际中心F座17层
邮政编码：610041
电话：+86 28 6789 8188
传真：+86 28 6317 3500

重庆
重庆市渝中区民族路188号
环球金融中心43层
邮政编码：400010
电话：+86 23 8823 1888
传真：+86 23 8857 0978

大连
大连市中山路147号
申贸大厦15楼
邮政编码：116011
电话：+86 411 8371 2888
传真：+86 411 8360 3297

广州
广州市珠江东路28号
越秀金融大厦26楼
邮政编码：510623
电话：+86 20 8396 9228
传真：+86 20 3888 0121

杭州
杭州市上城区飞云江路9号
赞成中心东楼1206室
邮政编码：310008
电话：+86 571 8972 7688
传真：+86 571 8779 7915

哈尔滨
哈尔滨市南岗区长江路368号
开发区管理大厦1618室
邮政编码：150090
电话：+86 451 8586 0060
传真：+86 451 8586 0056

合肥
安徽省合肥市蜀山区潜山路111号
华润大厦A座1506单元
邮政编码：230022
电话：+86 551 6585 5927
传真：+86 551 6585 5687

香港
香港金钟道88号
太古广场一座35楼
电话：+852 2852 1600
传真：+852 2541 1911

济南
济南市市中区二环南路6636号
中海广场28层2802-2804单元
邮政编码：250000
电话：+86 531 8973 5800
传真：+86 531 8973 5811

澳门
澳门殷皇子大马路43-53A号
澳门广场19楼H-L座
电话：+853 2871 2998
传真：+853 2871 3033

南昌
南昌市红谷滩区绿茵路129号
联发广场写字楼41层08-09室
邮政编码：330038
电话：+86 791 8387 1177
传真：+86 791 8381 8800

南京
南京市建邺区江东中路347号
国金中心办公楼一期40层
邮政编码：210019
电话：+86 25 5790 8880
传真：+86 25 8691 8776

宁波
宁波市海曙区和义路168号
万豪中心1702室
邮政编码: 315000
电话：+86 574 8768 3928
传真：+86 574 8707 4131

青岛
山东省青岛市崂山区香港东路195号
上实中心9号楼1006-1008室
邮政编码：266061
电话：+86 532 8896 1938

三亚
海南省三亚市吉阳区新风街279号
蓝海华庭（三亚华夏保险中心）16层
邮政编码：572099
电话：+86 898 8861 5558
传真：+86 898 8861 0723

上海
上海市延安东路222号
外滩中心30楼
邮政编码：200002
电话：+86 21 6141 8888
传真：+86 21 6335 0003

沈阳
沈阳市沈河区青年大街1-1号
沈阳市府恒隆广场办公楼1座
3605-3606单元
邮政编码：110063
电话：+86 24 6785 4068
传真：+86 24 6785 4067

深圳
深圳市深南东路5001号
华润大厦9楼
邮政编码：518010
电话：+86 755 8246 3255
传真：+86 755 8246 3186

苏州
苏州市工业园区苏绣路58号
苏州中心广场58幢A座24层
邮政编码：215021
电话：+86 512 6289 1238
传真：+86 512 6762 3338 / 3318

天津
天津市和平区南京路183号
天津世纪都会商厦45层
邮政编码：300051
电话：+86 22 2320 6688
传真：+86 22 8312 6099

武汉
武汉市江汉区建设大道568号
新世界国贸大厦49层01室
邮政编码：430000
电话：+86 27 8538 2222
传真：+86 27 8526 7032

厦门
厦门市思明区鹭江道8号
国际银行大厦26楼E单元
邮政编码：361001
电话：+86 592 2107 298
传真：+86 592 2107 259

西安
西安市高新区唐延路11号
西安国寿金融中心3003单元
邮政编码：710075
电话：+86 29 8114 0201
传真：+86 29 8114 0205

郑州
郑州市金水东路51号
楷林中心8座5A10
邮政编码：450018
电话：+86 371 8897 3700
传真：+86 371 8897 3710

关于德勤

德勤中国是一家立足本土、连接全球的综合性专业服务机构，由德勤中国的合伙人共同拥有，始终服务于中国改革开放和经济建设的前沿。我们的办公室遍布中国31个城市，现有超过2万名专业人才，向客户提供审计及鉴证、管理咨询、财务咨询、风险咨询、税务与商务咨询等全球领先的一站式专业服务。

我们诚信为本，坚守质量，勇于创新，以卓越的专业能力、丰富的行业洞察和智慧的技术解决方案，助力各行各业的客户与合作伙伴把握机遇，应对挑战，实现世界一流的高质量发展目标。

德勤品牌始于1845年，其中文名称“德勤”于1978年起用，寓意“敬德修业，业精于勤”。德勤全球专业网络的成员机构遍布150多个国家或地区，以“因我不同，成就不凡”为宗旨，为资本市场增强公众信任，为客户转型升级赋能，为人才激活迎接未来的能力，为更繁荣的经济、更公平的社会和可持续的世界开拓前行。

Deloitte（“德勤”）泛指一家或多家德勤有限公司，以及其全球成员所网络和它们的关联机构（统称为“德勤组织”）。德勤有限公司（又称“德勤全球”）及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。德勤有限公司及其每一家成员所和它们的关联机构仅对自身行为承担责任，而对相互的行为不承担任何法律责任。德勤有限公司并不向客户提供服务。请参阅www.deloitte.com/cn/about了解更多信息。

德勤亚太有限公司（一家担保责任有限公司，是境外设立有限责任公司的其中一种形式，成员以其所担保的金额为限对公司承担责任）是德勤有限公司的成员所。德勤亚太有限公司的每一家成员及其关联机构均为具有独立法律地位的法律实体，在亚太地区超过100个城市提供专业服务，包括奥克兰、曼谷、北京、班加罗尔、河内、香港、雅加达、吉隆坡、马尼拉、墨尔本、孟买、新德里、大阪、首尔、上海、新加坡、悉尼、台北和东京。

本通讯中所含内容乃一般性信息，任何德勤有限公司、其全球成员所网络或它们的关联机构并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合资格的专业顾问。

我们并未对本通讯所含信息的准确性或完整性作出任何（明示或暗示）陈述、保证或承诺。任何德勤有限公司、其成员所、关联机构、员工或代理方均不对任何方因使用本通讯而直接或间接导致的任何损失或损害承担责任。

Designed by CoRe Creative Services. RITM1636539

这是环保纸印刷品