中国太平洋财产保险公司厦门分公司文件

厦太保产发〔2024〕38号

关于印发修订后的《太平洋产险厦门分公司个人信息保护管理实施细则》的通知

各机构、各部（室）：

为落实《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中国银保监会关于印发银行保险机构消费者权益保护监管评价办法的通知》（银保监发〔2021〕24号）、《关于印发〈中国太平洋财产保险股份有限公司个人信息保护管理办法〉的通知》（太保产发〔2024〕111号）、《关于印发〈太平洋产险厦门分公司数据维护和提取管理办法（2020年版）〉的通知》（厦太保产发〔2020〕39号）等法律法规和监管

要求，加强分公司个人信息保护工作统筹管理和部署，压实个人信息保护主体责任，建立健全个人信息保护管理制度体系和工作机制，现将修订后的《太平洋产险厦门分公司个人信息保护管理实施细则》印发给你们，请认真学习并遵照执行。

特此通知。

中国太平洋财产保险股份有限公司

厦门分公司

2024年8月15日

太平洋产险厦门分公司个人信息保护管理实施细则

第一章　总则

第一条　为规范分公司个人信息处理活动，加强公司个人信息保护工作统筹管理，压实各级机构个人信息保护主体责任，完善个人信息保护在全生命周期的具体技术实施要求，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中国银保监会关于印发银行保险机构消费者权益保护监管评价办法的通知》（银保监发〔2021〕24号）、《关于印发〈太平洋产险厦门分公司数据维护和提取管理办法（2020年版）〉的通知》（厦太保产发〔2020〕39号）等法律法规和监管要求，特制订本细则。

第二条　本细则适用于各单位在中华人民共和国境内开展个人信息处理的活动，以及该活动所产生各类个人信息数据的安全保护和具体技术实施。

第二章　相关术语和定义

第三条　相关术语和定义

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，主要包括姓名、出生日期、证件号码、生物识别信息、住址、通信通讯联系方式、通讯记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等，不包括匿名化处理后的信息。

敏感个人信息：是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包

括生物识别、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。

个人信息主体：是指个人信息所标识或关联到的自然人。

个人信息的处理：包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

个人信息脱敏：是指对个人敏感信息进行数据变形，以实现保护个人隐私。

个人信息屏蔽：是指通过个人信息在网络中无法被检索、访问或泄露。

个人信息去标识化：是指个人信息经过处理，使其不借助额外信息的情况下无法识别或关联到特定自然人。

个人信息匿名化：是指个人信息经过处理，使其无法识别特定自然人且不能复原。

第四条　个人信息和个人敏感信息的范围依据国家标准《信息安全技术—个人信息安全规范》（GB/T35273-2020），如国家标准后续有更新，具体范围以国家标准的最新版本为准。

第三章　个人信息保护管理原则

第五条　个人信息保护遵循合法、正当、必要和诚信的原则，符合法律法规、监管及行业的各项规定，具体包括：

（一）合法合规原则：应满足国家法律法规及行业主管部门有关规定，采取技术和其它必要的措施保障个人信息安全。

（二）最小必要原则：在保证组织业务功能完整实现的基础上应赋予数据使用过程中各角色最小的访问、操作权限，落实授权审批流程和操作留痕，实现异常操作行为的有效监控和干预。

（三）最大保护原则：个人信息安全须从制度、流程、信息技术等环节持续完善，最大程度保护个人信息安全。接触个人信息的岗位人员应对相关个人信息负有安全保护责任，不得擅自篡改、记录、泄露。

（四）公开透明原则：以明确、易懂和合理的方式公开个人信息处理规则，明示处理的目的、方式和范围，并接受外部监督。

第六条　不得非法收集、使用、加工、传输个人信息，不得非法买卖、提供或者公开个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

第四章　管理职责和责任分工

第七条　按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，落实个人信息处理时的各项主体责任和安全要求。

第八条　分公司数据管理专项工作委员会是个人信息保护工作的牵头组织，负责统筹分公司个人信息保护相关管理工作，拟定个人信息保护管理实施细则，其主要职责包括:

（一）拟定个人信息保护管理实施细则，统筹建立个人信息安全事件应急管理机制，组织开展个人信息保护宣贯培训;

（二）组织推动公司开展个人信息分类分级管理工作;

（三）组织开展个人信息保护相关法律法规、制度、流程执行情况的检查与评估工作;

（四）推动健全个人信息防护体系，监督个人信息问题的整改落实。

第九条　分公司信息技术部是个人信息保护工作的技术部保护主责部门，其主要职责包括:

（一）建立个人信息技术保护体系，建立个人信息保护技术架构和保护控制基线，落实技术保护措施;

（二）制定个人信息保护技术标准规范，组织开展个人信息保护技术风险评估;

（三）组织开展信息系统的生命周期安全管理，采取相应的加密、去标识化等安全技术措施，确保个人信息保护措施在需求、开发、测试、投产、监测等环节得到落实;

（四）建立个人信息保护技术应急管理机制，组织开展个人信息保护风险技术监测、预警、通报与处置，防范外部攻击行为;

（五）组织个人信息保护技术研究与应用。

第十条　分公司各条线或部门按照“谁管业务、谁管业务数据、谁管数据安全”的原则，是其主管领域个人信息安全的业务主责部门，负责个人信息保护管理制度、方案和流程在本部门的落地实施。

个客中心综合市场部、团客中心综合市场部、三农中心综合市场部为各条线内个人信息保护工作的业务牵头部门，负责统筹条线内个人信息保护管理工作，将个人信息保护管理要求融入条线内业务管理的各项制度并推动落地。

第十一条　个人保证保险事业部厦门门店遵循总部个人信用信息基础数据库管理，做好个人信用信息基础数据库对接工作并配合分公司其他部门做好个人信息保护工作。

第十二条　人力资源部作为员工个人信息的归口管理部门，统筹各条线部门做好员工个人信息保护相关工作；负责与接触个人信息的人员签订保密协议，明确保密责任。

第十三条　运营服务部作为消保审查统筹管理部门，负责根据《关于印发〈太平洋产险厦门分公司消费者权益保护审查工作管理实施细则〉的通知》（厦太保产发〔2024〕4号）开展消费者权益保护审查，在产品和服务开发设计早期有效识别风险，保护消费者信息安全权。

第十四条　法律合规部是个人信息保护的合规内控检查部门，组织开展个人信息保护相关法律法规、制度、流程执行情况的检查与评估工作，对个人信息安全方面的协议、合同及保密协议书等进行法律审核，提供法律合规意见，确保个人信息保护措施符合相关法律法规和政策规定。

第十五条　分公司各部门负责落实分公司个人信息保护管理各项要求，负责本部门个人信息保护管理工作的推进落实，定期梳理个人信息处理的操作权限，并定期对从业人员进行安全教育和培训，强化保密意识。

第五章　个人信息收集

第十六条　各业务条线应结合通用隐私政策、业务场景制定个人信息收集格式条款或业务场景隐私政策，并在信息收集前进行明

示，内容包括但不限于收集个人信息使用目的、方式、范围、种类、保存期限等规则。法律合规部、消费者权益保护管理部门对制定的收集格式条款或业务场景隐私政策分别进行法律审核和消费者权益保护审查。

第十七条　公司收集个人信息除法律、行政法规另有规定外，应当经个人信息主体同意。个人信息主体不同意的，公司不得因此拒绝提供不依赖于其所拒绝授权信息的产品或服务。

公司不得采取变相强制、违规购买等不正当方式收集使用个人信息。

第十八条　各业务条线是个人信息保护合规的第一道防线，应确保合作方收集个人信息是合法合规的，在签署合作协议时应包含有对个人信息的信息来源合法性与授权完整性的承诺。同时加强对合作机构收集处理投保人、被保险人、受益人以及业务活动相关当事人个人信息的行为管控，充分评估合作机构信息系统服务能力、可靠性和安全性以及敏感数据的安全保护能力，在双方合作协议中明确信息收集处理行为要求，定期了解执行协议要求情况，发现存在违反协议要求情形时，应及时采取措施予以制止和督促纠正，并依法追究该机构责任，视情节严重程度和协商情况予以清退，列入合作机构风险控制名单。

第十九条　公司应用系统、APP和小程序等在个人信息收集的实施要求:

（一）将审定过的协议、合同或制度等嵌入到系统中，并在显目位置体现;

（二）基于上述格式条款或个人隐私政策提供拒绝、撤回同意功能;

（三）系统收集到用户的授权同意时应记录授权状态、时间、方式、类型等;

（四）收集全过程应有相应的日志记录，保存至少 180 天;

（五）使用第三方组件时，应避免第三方组件未经授权收集客户端应用软件信息和个人信息;

（六）不得出现《App违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191 号）所明确的禁止性行为。

第二十条　公司三方对接系统和合作数据在个人信息收集的实施要求:

（一）制定并定期更新接口文档，明确收集个人信息字段、调用方式、参数说明、返回值等信息，以便第三方系统能正确使用和调用;

（二）确保接口调用安全性，使用身份认证、访问权限等方式。

第六章　个人信息存储

第二十一条　公司在境内收集和产生的个人信息须存储在境内。

第二十二条　各业务条线对纸质类个人信息应建立纸质档案管理制度，包括但不限于分类、编号、存储、保管、使用等方面规定。

第二十三条　公司员工个人终端仅能存储完成工作任务所必须的最小范围的敏感个人信息，不得用于任何非工作相关的用途，在完成相关工作任务后应及时删除。

第二十四条　公司应用系统、APP和小程序等在个人信息存储的实施要求:

（一）存储个人信息应使用符合国家密码标准的加密方式进行加密，确保数据存储安全性;

（二）APP涉及存储个人生物识别信息的应与个人身份信息分开存储;

（三）APP客户端本地不能明文保存用户敏感数据（如密码、卡号、证件号等），应采用国密算法加密后再保存。

第二十五条　存储三方对接系统或合作数据应额外记录数据来源信息，如包含第三方名称、数据有效期、授权情况等。

第七章　个人信息使用、加工

第二十六条　个人信息应在数据收集时所声明的目的、范围、处理方式内使用，应当按照“业务必要授权”原则，对个人信息实施授权管理，建立与其安全等级相匹配的审批机制，并对数据访问行为实施审计。

第二十七条　各业务条线对已取得个人同意所采集的个人信息享有分析、应用的使用权和数据安全责任。

第二十八条　公司应用系统、APP、小程序、三方对接系统和合作数据在个人信息使用、加工的实施要求:

（一）涉及个人信息访问的系统应设置身份验证和授权机制，如使用强密码以及双因素验证等方式来验证用户身份;

（二）应用系统、APP和小程序等涉及数据前台界面展示的，应对个人敏感信息进行脱敏处理（如屏蔽、去标识、匿名化等），防

止内部非授权人员及客户之外的其他人员未经授权获取个人信息，降低个人信息在展示环节的泄露风险;

（三）应用系统、APP和小程序等涉及数据导出下载的，应建立审批流程以及双因素认证机制，导出的数据须经脱敏;

（四）通过后台查询数据的，应通过技术手段（如动态脱敏等）对展示的个人敏感信息进行脱敏处理;

（五）开发环境、测试环境不应使用真实个人信息数据，以免造成数据泄露，如测试需要应使用数据脱敏平台软件或编写脱敏规则进行脱敏;

（六）对个人信息数据访问、导出与增删改查等操作进行记录，保证操作日志的完整性、可用性及可追溯性，操作日志包括但不限于业务操作日志、系统日志等；系统运维管理类日志不应记录个人敏感信息。所有日志保留不少于180天;

（七）具有登录功能的互联网系统，在涉及敏感信息时（包括但不限于：身份证号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等），应设置会话超时不得大于15分钟。应用会话超时后，二次认证可选择重新登录。

第八章　个人信息传输

第二十九条　公司员工须遵守《关于印发〈中国太平洋保险（集团）股份有限公司数据防泄漏管理办法〉的通知》（太保发〔2022〕105号），不得将公司所属的个人信息通过邮件、INTERNET访问、打

印、移动存储介质、FTP、文件共享、即时通信软件、蓝牙等任何传输渠道非法传输到公司外部。

第三十条　公司应用系统、APP、小程序、三方对接系统和合作数据在个人信息传输的实施要求:

（一）互联网传输应采用VPN链路加密或HTTPS（应采用TLS1.2及1.2以上版本加密）;

（二）对于互联网传输的敏感信息应采取加密方式传输，如用户名、密码、卡号、ID等。请求中含有敏感参数（如订单号、ID等),应加密处理后传输，防止产生参数遍历获取信息风险;

（三）应用系统间数据传输应建立点对点的控制，防止未授权的数据传输。

第九章　个人信息提供

第三十一条　公司任何员工不得非法买卖、提供他人任何个人信息。未经个人同意，不得向他人提供该个人的信息，法律法规规章另有规定以及开展保险业务所必需的除外。

第三十二条　公司需提供个人信息的应进行个人信息保护影响评估，并对处理情况进行记录，相关评估报告和记录应至少保存三年，评估要包含以下方面:

（一）提供个人信息的目的、方式等是否合法、正当、必要;

（二）对个人权益的影响及安全风险;

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

第三十三条　各业务条线与第三方合作时应签署保密协议，约定个人信息收集范围、数据保护责任、保密时间、保密义务、监督、

处罚、合同终止和突发情况下的应急处置条款，明确个人信息使用的范围，包括信息内容、信息数量、信息使用目的、时间和范围，确定个人信息传递方式、第三方信息管理责任人及其责权，且要确认合作机构所有的个人信息为合法来源。

第三十四条　公司三方对接系统和合作数据在个人信息提供的实施要求:

（一）评估并确保合作机构具备足够的数据安全防护能力;

（二）通过专用线路、物理隔离、数据加密、权限管控、监测报警、去标识化等方式，严格控制合作机构行为与权限，防范数据滥用或者泄露风险。

第十章　个人信息公开

第三十五条　公司公开个人信息应得到个人的单独同意，同时对公开的个人信息敏感字段进行脱敏。

第十一章　个人信息删除

第三十六条　公司应明示个人信息授权撤回，注销应用系统、APP、小程序等账号，删除个人信息的申请路径，并依法依约提供或支持相应的服务。

第三十七条　公司对个人撤回同意、注销账号、三方提供数据超出有效期等，或依据法律法规规定提出删除个人信息的，应及时删除其个人信息，且删除应采用不可恢复的模式，经过处理无法关联到特定个人且不能复原（匿名化处理）的除外。

第十二章　个人信息保护安全处置

第三十八条　如发生个人信息泄露、篡改、丢失的，按照《关于印发修订后〈中国太平洋保险（集团）股份有限公司网络安全事件应急预案〉的通知》（太保发〔2022〕109号）中网络安全事件分类为信息破坏事件和信息内容安全事件的处置方式处理，并立即通知履行个人信息保护职责的部门，及时采取补救措施。通知应当包括下列事项:

（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、数量、原因和可能造成的危害;

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施;

（三）个人信息处理者的联系方式。

第三十九条　如发生个人征信信息安全事件的应按照公司《关于印发〈中国太平洋财产保险股份有限公司个人征信信息安全事件应急预案〉的通知》（太保发〔2018〕168号）进行处置。

第四十条　为确保公司应用系统、APP和小程序等不发生因系统安全漏洞缺陷导致的信息泄露，如未授权、越权、SQL注入、敏感信息未脱敏等漏洞，投产前应进行安全漏洞扫描，修复完成后方可上线；投产后应定期开展全盘安全漏洞扫描，对发现的漏洞问题在修复时效内完成修复。

第四十一条　采取有效的技术手段防止个人信息泄露的发生，如使用防火墙、入侵检测等安全技术或设备对网络进行隔离和保护，防止未经授权访问和数据泄露引发个人信息安全事件，以及通过安

全监控和告警系统，实时监测和预警网络安全事件和攻击行为，及时发现和处理个人信息安全问题。

第四十二条　所有个人办公终端应安装数据防泄漏系统，避免个人信息通过个人终端发生外泄。

第四十三条　公司统一使用集团账号权限管理系统对涉及处理使用个人信息的业务信息系统进行分级授权审批工作，各业务和信息系统的主管部门遵循权责对应、最小必要原则设置访问、操作权限，落实授权审批流程，对异常操作行为进行有效监控和干预。

第十三章　投诉与问责

第四十四条　公司任何员工严禁利用岗位权限，违规查询、修改、下载及使用个人信息，严禁通过网络传输、拷贝、打印、复印、拍照、截图等方式泄露、兜售及倒卖个人信息。

第四十五条　对引发相关高频投诉的，事发部门应自发生之时起 2 小时内向分公司运营服务部进行报告，最大程度减少事件造成的负面影响。

第四十六条　对违反本细则相关要求，符合问责规定的，根据公司问责相关工作要求，对责任人、责任机构予以问责；涉嫌犯罪的，依法移送司法机关追究相关人员刑事责任，并按照公司涉刑案件管理办法履行报告职责。

第十四章　附则

第四十七条　其他未尽事宜参照国家有关的法律法规、监管规定及公司相关制度执行。

第四十八条　本细则由分公司数据管理专项工作委员会负责解释。

第四十九条　本细则自发文之日起实施。原《关于印发〈太平洋产险厦门分公司个人信息保护管理办法〉的通知》（厦太保产发〔2021〕65号）即时废止。

中国太平洋财产保险公司 厦门分公司办公室	2024年8月15日 印发
编录：曾秀玲	校对：邱丹丹