复星旅文集团
个人信息保护制度

LC_T_LC•00_005_V2.0

Fosun Tourism Group 2022-8-23 首次发布
2024-1-4 更新发布

FOSUN Holiday 复星旅文

版本	修改日期	修改摘要	修改人	审批日期
V1.0	2022.8.23	首次发布	-	2022.8.23
V2.0	2024.1.4	更新发布	-	2024.1.4

FOSUN Holiday 复星旅文

目录

1.目的

为了落实个人信息处理者义务，规范复星旅文集团及其所有下属公司（“公司”）个人信息处理活动，防止个人信息被篡改、泄露、窃取等事件发生，特制定本制度。

2.适用范围

适用于公司所有企业。公司内各企业如共享数据，则共同承担相关个人信息处理者的责任。

3.定义

3.1 个人信息：个人信息是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，不包括匿名化处理后的信息。

3.2 敏感个人信息：敏感个人信息是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。

4.个人信息保护原则

个人信息的保护应当遵循以下原则：

1）**合法收集**：不得欺诈、诱骗、强迫个人信息主体提供其个人信息，不得隐瞒产品或服务所具有的收集个人信息的功能，不得从非法渠道获得个人信息，不得收集法律法规明令禁止收集的个人信息。

2）**目的明确**：处理个人信息应当具有明确、合理的目的，并应当与处理目的直

接相关，采取对个人权益影响最小的方式。

3）**最小必要**：收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

4）**知情同意**：处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围，并获得个人信息主体的授权同意；个人信息的处理目的、处理方式和处理的个人信息种类发生变更时，应当重新取得个人同意；处理敏感个人信息应当取得个人信息主体的单独同意。

5）**质量保证**：处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

6）**安全保障**：具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

7）**主体参与**：向个人信息主体提供能够查询、复制、更正、转移、删除、限制处理、注销账户、撤回授权、投诉的途径和方法。

5.组织管理

5.1 公司法定代表人对个人信息安全负全面领导责任，包括为个人信息安全工作提供人力、财力、物力保障等。

5.2 个人信息保护负责人：公司信息安全官为公司个人信息保护负责人。公司个人信息保护负责人的职责包括：

5.2.1 全面统筹实施公司内部的个人信息安全工作，对个人信息安全负直接责任。

5.2.2 制定数据合规管理整体方针策略，协调建立数据合规技术保障措施，牵头做好数据风险识别、风险评估、风险处置等工作。

5.2.3 审核评估企业的经营管理和业务行为，确保与供应商、代理商、经销商、关联企业、分支机构的业务活动，以及处理个人信息等活动符合数据法规的要求，并制定数据风险应对措施。

5.2.4 制定、签发、实施、定期更新隐私政策和相关规程。

5.2.5 建立、维护和更新公司所持有的个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略。

5.2.6 开展个人信息安全影响评估。

5.2.7 组织开展个人信息安全培训。

5.2.8 在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为。

5.2.9 进行个人信息安全审计。

5.2.10 建立个人信息保护团队。

5.2.11 与监督、管理部门保持沟通，通报或报告个人信息保护和事件处置等情况。

5.3 所有员工对其他员工、客户或其他个人信息负保密义务。

6.个人信息处理全流程管理

公司处理用户个人信息，应遵循以下原则：权责一致原则、目的明确原则、选择同意原则、最少够用原则、公开透明原则、确保安全原则、主体参与原则，切实落实网络安全义务，保障用户权利，确保个人信息安全。

6.1 个人信息收集

6.1.1 合法性要求

1）不得欺诈、诱骗、强迫个人信息主体提供其个人信息。

2）不得隐瞒产品或服务所具有的收集个人信息的功能。

3）不得从非法渠道获得个人信息。

4）不得收集法律法规明令禁止收集的个人信息。

6.1.2 最小化要求

1）收集的类型应与实现产品或服务的业务功能直接相关。

2）自动采集的频率应为实现产品或服务的业务功能所必需的最低频率。

3）获取的数量应为实现产品或服务的业务功能所必需的最少数量。

6.1.3 授权同意

1）直接获取：向用户明确告知所提供产品或服务的不同业务功能分别收集的个人信息类型，以及收集、使用个人信息的规则，并获得用户的同意。按照服务类型分别向个人申请处理个人信息的同意，不得使用概括性条款取得同意。

2）间接获取：要求提供方说明个人信息来源，确认来源的合法性；审查授权同意范围，用户是否授权同意共享或转让等。

6.1.4 收集个人敏感信息单独明示同意

1）处理个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息应当取得个人单独同意；

2）处理不满十四周岁未成年人的个人信息，应当取得其监护人同意；

明示同意的方式包括签字同意、行动同意、主动勾选、主动点击“同意”、“注册”、“发送”等。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意，并同步修改个人信息处理规则。

6.1.5 收集个人信息采取的安全技术措施

1）去标识化：收集个人信息后，应立即进行去标识化处理，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

2）数据打标：收集后的个人信息，根据公司内部的分类分级管理制度，进行相应分类分级并打标，实现对收集的数据字段级别的分类分级管理。

6.1.6 个人信息收集行为的监督

1）验证数据的真实性、准确性，并定期对数据质量进行分析和监控，及时对异常数据进行告警修正；

2）跟踪和记录数据收集过程，保证数据收集活动的可追溯性。

6.2 个人信息使用

6.2.1 员工和企业开展数据处理活动应当遵守法律、行政法规，尊重社会公德和伦理，不得从事以下活动：

1）危害国家安全、荣誉和利益，泄露国家秘密和工作秘密；

2）侵害他人人格权、知识产权和其他合法权益等；

3）通过窃取或者以其他非法方式获取数据；

4）非法出售或者非法向他人提供数据；

5）制作、发布、复制、传播违法信息；

6）法律、行政法规禁止的其他行为。

6.2.2 除目的所必需外，使用个人信息时应通过使用用户身份证明、敏感信息掩码等方式进行去标识化处理，消除明确身份指向性，避免精确定位到特定个人。

6.2.3 不得超出与收集时声称的目的具有直接或合理相关的范围，否则应再次征得同意。

6.2.4 对所收集的个人信息加工处理而产生的信息，如可认定为个人信息的，对其处理应遵循收集时获得的授权同意的范围。

6.2.5 个人信息使用的监督与审批

对个人信息的使用，应通过日志分析，分析异常行为，进行有效的识别、监控和预警。

对个人信息的重要操作行为，须通过内部审批流程，确保数据使用行为的安全可控。

6.2.6 个人信息使用的访问控制措施

建立统一的身份和访问管理平台，采取多因子认证、口令管理等技术措施，提供和实施对数据的细粒度访问控制机制，限定用户可访问数据范围，防止数据非授权的泄露、篡改和损坏。

6.2.7 敏感个人信息的处理

敏感个人信息的处理应与特定的处理目的密切相关，应符合非必要不处理的原则。

在处理敏感个人信息前，应进行个人信息保护影响评估。在处理时应对处理过程进行记录，以保障处理敏感个人信息流程合法合规。

6.2.8 已公开个人信息的处理

对已公开个人信息进行处理时：

1）不应向已公开个人信息中的电子邮件、手机号码等发送与其公开目的无关的信息；

2）不应利用已公开的个人信息从事网络暴力活动；

3）不应处理个人明确拒绝处理的已公开个人信息。

6.3 个人信息存储

6.3.1 保存时间最小化

个人信息保存期限应为实现目的所必需的最短时间，保存期限届满后应进行删除或匿名化处理。

6.3.2 个人信息加密存储要求：

1）存储个人敏感信息时，应采用加密等安全措施；

2）个人生物识别信息应与个人身份信息分开存储；

3）原则上不应存储原始个人生物识别信息（如样本、图像等），如需存储，应采取以下措施：

a) 仅存储个人生物识别信息的摘要信息；

b) 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；

c) 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

6.3.3 电子化的个人信息应储存在安全的公共云盘中。云盘密码长度不得低于 6 位，密码须由数字和字母组成，密码有效期为 90 天，且新密码不得与前 2 次的密码一致。

纸质文档个人信息应由专人保管在可以上锁的安全场所，且应保存在安全的物理环境下（如：防火、电力、空调、湿度、静电及其他环境保护措施）。员工个人不得私自保存、使用公司所收集、管理存储的个人信息。对个人信息所在的数据中心的运维人员建立严格管理制度，对所有运维人员进行安全背景审查。

6.4 个人信息的共享与转让

6.4.1 除征得用户授权同意外，公司不得向外共享、转让个人信息。如根据业务发展要求，确需共享、转让个人信息的，应遵守以下要求：

1）根据共享、转让个人信息的类型、规模，由个人信息安全负责人决定是否事先开展个人信息影响评估，并依评估结果采取有效的保护用户的措施。

2）向个人告知提供个人信息的目的、类型、方式、范围、存储期限、存储地点，以及接收方的名称或者姓名、联系方式、处理目的、处理方式，并取得个人单独同意，符合法律、行政法规规定的不需要取得个人同意的情形或者经过匿名化处理的除外；

3）共享、转让个人敏感信息，除 2)中告知的内容外，还应向用户告知数据接收方的数据安全能力，并事先征得用户的明示同意。法律、行政法规规定应当取得书面同意的，应事先取得用户书面同意。

4）准确记录和保存个人信息共享、转让的情况，包括共享、转让的日期、规模、目的以及数据接收方基本情况等。

5）帮助用户了解数据接收方对个人信息的保存、使用等情况，以及用户的权利。

6）与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督；变更处理目的、范围、方式时，应重新取得用户的单独同意。

7）留存个人同意记录及提供个人信息的日志记录，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。

6.4.2 数据传输时，应采取以下技术措施：

1）传输过程中，采用数据传输加密 SSL/TSL 协议，应用层对于敏感数据进行应用层对称数据加密，以保障数据传输的完整性和安全性；

3）HTTP/HTTPS 请求中包含用户敏感信息的，必需使用 POST 方式，禁止通过 GET 方式；

4）禁止敏感信息进行落地的导入导出，只能通过 API 数据接口进行数据流转；

5）涉及包含敏感信息文件的传输必须使用专用的文件交换系统进行处理。

6）对于金融卡信息（银行卡号、CVV、有效期）应采取字段级加密手段，防止信息泄漏。

6.4.3 为保障传输接口的安全性，应采取以下措施：

1）建立设备准入机制，通过 MAC 地址、IP 地址或端口号绑定等方式进行设备准入。

2）建立数据传输流程控制机制，记录关键操作日志，制定接口契约，包括接口名称、接口参数及接口安全要求等。

3）建立接口安全监控机制，梳理敏感接口并形成清单，监控所有数据传输接口的使用情况，监控敏感接口及低活跃接口，识别异常访问，及时下线废置接口，提升接口安全性。

6.5 个人信息的公开披露

6.5.1 个人信息原则上不应公开披露。若经法律授权或具备合理事由确需公开披露时，应遵守以下要求：

1）事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

2）向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意；

3）公开披露敏感个人信息前，除 2)中告知的内容外，还应向个人信息主体告知涉及的敏感个人信息的内容；

4）准确记录和存储个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等；

5）不应公开披露个人生物识别信息；以及

6）不应公开披露种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果。

6.5.2 针对确需要公开或展示的个人信息，应根据不同数据类型采取不同的安全技术措施，具体包括：

1）常用联系人、用户个人信息默认展示时隐藏处理；

2）除生成订单和等待支付状态外，其他订单状态（如订单取消、订单查询）应将电话号码、邮箱、银行卡、身份证号码信息进行隐藏处理；

3）证件号前 4 位至后 3 位之间隐藏处理，手机号码前 3 位至后 4 位之间隐藏处理，邮箱名前 3 位至@之间隐藏处理（邮箱名小于等于 3 位时，邮箱名第 1 位至@之间的隐藏处理），银行卡信息后 4 位以外隐藏处理，座机电话号码从最后 2 位开始向后隐藏 3 位；

4）护照/港澳通行证/台胞证/回乡证/国际海员证/大陆居民往来台湾通行证等，前 2 位至后 2 位之间隐藏处理；

5）隐藏实现方式必须在后端进行处理，禁止在前端处理。

6.5.3 定期更新和评估已公开的数据，对不适宜继续公开或超出公开期限的数据进行召回或销毁处理。

6.5.4 承担因公开披露个人信息对个人信息主体合法权益造成损害的相应责任。

6.6 个人信息的删除

6.6.1 个人信息删除的情形

以下情形时，应对个人信息进行删除或匿名化处理：

1）在超出实现目的所必需的最短期限，法律法规及监管规定的数据存储期限；

2）个人信息处理目的已实现、无法实现或者为实现处理目的不再必要；

3）个人信息主体行使删除权；

4）个人信息主体注销账户；

5）个人信息主体撤回同意；

6）因使用自动化采集技术等，无法避免采集到的非必要个人信息或者未经同意的个人信息。

6.6.2 个人信息删除要求

1）公司设立个人信息删除评估与审批程序，对拟删除数据的范围、删除理由、再利用的可能性等进行评估，经公司数据安全负责人批准后实施数据删除；

2）提供数据删除技术措施和工具，对批准后的重要数据及其副本进行删除，包括数据处理过程中备份数据、衍生数据及操作日志数据等，确保删除后的数据以商业手段不可恢复；

3）建立数据删除效果评估机制，定期检查删除措施的有效性；

4）对数据删除过程留存日志，记录数据删除的审批、实施过程，以及被删除数据的具体情况；

5）在存储介质上删除机密信息时，执行安全删除与格式化，或重复写操作防止已删除数据的恢复；

6）若需要将存储介质提供给第三方使用，存储介质管理员需要确认机密信息已经安全删除。

6.7 个人信息出境

6.7.1 如涉及个人信息出境，应征得用户单独同意。

6.7.2 个人信息出境，应按法律法规要求，结合本制度相关规定，进行个人信息影响评估，需得到公司、信息安全负责人的审批。数据出境安全评估应重点考虑以下内容：

1）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

2）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

3）境外接收方承诺承担的责任义务，以及履行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；

4）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

5)与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务。

6.7.3 存在以下情况之一的，个人信息不得出境：

1）未取得个人信息主体单独同意，且不存在其他法定合法性基础的；

2）数据出境将导致国家政治、经济、科技、国防安全产生风险，可能影响国家安全，损害社会公共利益的；

3）其他经国家网信部门、公安部门等主管部门认定不得出境的。

6.8 用户权利保障

应建立便捷的方式和途径，接受、处理用户的个人信息主体权利，在接到用户的个人信息权利请求时，应及时响应并在合理的时间内进行处理。用户应享有的个人信息主体权利至少包括：

6.8.1 访问权

1）提供用户实现访问个人信息的方式。

2）访问的信息包括以下内容：公司所持有的关于该主体的个人信息或类型；上述个人信息的来源、所用于的目的；已经获得上述个人信息的第三方身份或类型。

6.8.2 复制权

提供用户复制个人信息副本的方式。

6.8.3 更正权

提供用户请求更正或补充信息的方式。

6.8.4 转移权

用户有权要求将其个人信息转移至其他平台、企业或组织。当用户请求转移个人信息时，公司应审核其请求，审核通过后，应在符合国家网信部门规定的条件下，向用户提供转移其相应个人信息的途径。

6.8.5 删除权

用户有权要求：

1）公司删除其个人信息。

2）向第三方共享、转让个人信息的，公司应立即停止共享、转让行为，并通知第三方及时删除。

3）公开披露个人信息的，公司应立即停止公开披露行为，并发布通知要求接收方及时删除。

6.8.6 限制处理权

提供用户限制信息系统、算法在内的非人工自动化决策机制处理其个人信息的方式。用户有权要求公司对自动化决策机制的处理规则进行说明。

6.8.7 撤回同意

提供用户撤回同意收集、使用个人信息的方式，用户撤回后公司不得再处理相应的个人信息。

6.8.8 注销账户

提供用户注销账户的方式，用户注销后应删除其个人信息或做匿名化处理。

7.隐私政策管理

7.1 隐私政策的基本要求

7.1.1 隐私政策独立、易读

1）隐私政策单独成文。

2）网站主页/App 主功能页面，4 次点击以内可访问；且链接位置突出、无遮挡。

3）隐私政策文字显示方式（字号、颜色、行间距等）不会造成阅读困难。

7.1.2 清晰说明各项业务功能及其收集个人信息类型

1）明示收集个人信息的业务功能，并逐项列举。

2）明示各项业务功能所收集的个人信息类型，并逐项列举。

3）业务功能与收集个人信息的类型一一对应。

4）显著标志个人敏感信息。

7.1.3 清晰说明个人信息处理规则及用户权益保障

1）运营者的基本情况，包括公司名称、注册地址、个人信息保护负责人的联系方式。

2）个人信息的使用规范，例如应用场景和可能对用户产生的影响。

3）个人信息的出境情况，逐项列举出境个人信息的类型并显著标识。

4）个人信息安全保护措施和能力，可说明已采取的措施（例如建立个人信息保

护制度、个人信息安全培训、个人信息授权策略等）、具备的能力（例如身份鉴别、数据加密等）、取得的资质（例如通过等保三级测评、App 安全认证等）。

5）对外共享、转让、公开披露个人信息的规则，包括目的、涉及个人信息的类型、接收方的类型或身份。

6）用户权利保障机制，明确说明用户查询、复制、更正、转移、删除、限制处理、注销账户、撤回授权的具体操作方法。

7）用户申诉渠道和反馈机制。

7.1.4 不应在隐私政策中设置不合理条款

不应设置免除自身责任、加重用户责任、排除用户主要权利条款。

7.1.5 隐私政策的发布

1）隐私政策时效，明确标识隐私政策发布、生效、更新日期。

2）隐私政策更新，包括更新的情形、方式（尽量能够直接通知到用户个人）。

7.2 隐私政策的制定、评审、发布、落实

7.2.1 制定

隐私政策由智能科创制定，产品、开发、运营、设计、法务等人员对隐私政策提供意见和建议。

7.2.2 发布

隐私政策由个人信息保护负责人签发，并在网站和 App 上发布。隐私政策发布应通过公告、电子邮件、信函、电话、推送通知等方式及时告知用户。

7.2.3 落实

隐私政策发布后，公司各部门应通力协作，确保隐私政策落地实施。

8.员工权限管理

8.1 内部个人信息操作人员

8.1.1 公司应根据职位需求，按照最小授权原则，分配内部个人信息操作人员权限。即个人信息操作人员职能访问职责所需的最少够用的个人信息，且仅具备完成职责所需的最少的数据操作权限。

8.1.2 每个职能部门及每个孵化企业，应明确内部个人信息操作权限，并指定个人信息保护专员，负责本部门或本企业的个人信息保护事项，管理本部门或本企业的个人信息。

8.1.3 内部数据操作岗位人员添加、变更、删除，应由部门最高领导审批，报个人信息保护负责人备案；内部数据操作岗位权限添加、变更、删除，应由个人信息保护负责人审批。

8.2 内部审批流程

对个人信息的重要操作，例如批量修改、拷贝、下载、删除等，应按照最小授权原则，经本部门或企业负责人，以及个人信息保护负责人审批。

内部审批流程变更，由个人信息保护负责人审批。

8.3 超权限处理

如确因工作需要，需授权特定人员超权限处理个人信息的，由个人信息保护负责人审批，并记录在册。

8.4 个人信息保护关键岗位

各部门及各孵化企业负责人，各个人信息保护专员，以及具有批量处理个人信息权限的员工，为个人信息保护关键岗位。关键岗位员工应严格保管个人信息存储管理密钥，并严格保密个人信息。关键岗位员工离职前应完成密钥交接。

9.个人信息安全影响评估

为了发现、处置和持续监控个人信息处理过程中的安全风险，根据业务现状、威胁环境、法律法规、标准要求等情况持续修正个人信息保护边界，调整安全控制措施，使个人信息处理过程处于风险可控的状态，公司应定期进行个人信息安全影响评估。

9.1 评估情形

1）法律法规有新的要求时。

2）业务模式、信息系统、运行环境发生重大变更时。

3）发生重大个人信息安全事件时。

4）除上述情形外，定期（每年一次）开展评估工作。

9.2 评估责任主体

个人信息安全影响评估由个人信息保护负责人启动并负责。个人信息保护负责人应确保评估流程的执行及结果的质量，签署评估报告。

9.3 评估内容

个人信息安全影响评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响。内容应至少包括：

1）个人信息收集环节是否遵循目的明确、知情同意、最小必要等原则；

2）个人信息处理是否可能对个人信息主体合法权益造成不利影响，包括是否会危害人身和财产安全、损害个人名誉和身心健康、导致差别性待遇等；

3）个人信息安全措施的有效性；

4）匿名化或去标识化处理后的数据集重新识别出个人信息主体或与其他数据集汇聚后重新识别出个人信息主体的风险；

5）共享、转让、公开披露个人信息对个人信息主体合法权益可能产生的不利影

响；

6）发生安全事件时，对个人信息主体合法权益可能产生的不利影响。

10.个人信息安全事件处置

10.1 如发生个人信息泄露、篡改、丢失等事件的，应当立即采取补救措施。安全事件涉嫌犯罪的，应当及时向公安机关报案。

10.2 及时上报

10.2.1 如发生任何个人信息安全时间，应立即上报个人信息安全负责人和风控官。

10.2.2 上报内容包括以下部分：

1）涉及个人信息主体的类型、数量、内容、性质等总体情况。

2）事件可能造成的影响。

3）已采取或将要采取的处置措施。

4）事件处置相关人员的联系方式。

10.3 及时披露

10.3.1 发生个人信息安全事件，除公司采取措施能够有效避免信息泄露、篡改、丢失造成的危害的情况外，应及时将事件情况以邮件、电话、推送通知等方式告知受影响的用户。难以逐一告知用户时，应采取合理、有效的方式发布与公众有关的警示信息。

10.3.2 告知内容包括以下部分：

1）安全事件的内容和影响。

2）已采取或将要采取的处置措施。

3）用户自主防范和降低风险的建议。

4）针对用户提供的补救措施。

5）个人信息保护负责人的联系方式。

11.个人信息安全审计

个人信息安全审计的内容应至少包括：

1）对个人信息保护政策、相关规程和安全措施的有效性进行审计；

2）建立自动化审计系统，监测记录个人信息处理活动；

3)审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑；

4）防止非授权访问、篡改或删除审计记录；

5）及时处理审计过程中发现的个人信息违规使用、滥用等情况；

6）审计记录和留存时间符合法律法规的要求。

12.个人信息安全责任培训

12.1 培训制度：

1）公司员工必须参与公司的全员个人信息保护培训；

2）鼓励员工参加其他行业和部门举办的专业培训，鼓励员工参加其他业务交流和学习培训；

3）鼓励员工结合业务、工作自学。

12.2 培训内容：

1）个人信息保护、数据安全、信息安全、网络安全等相关法律法规；

2）公司个人信息保护规章制度；

3）针对不同岗位的专题培训；

4）针对安全事件出现频率较高的业务线的专题培训。

12.3 培训周期：

1）每年至少举行一次全公司性质的个人信息保护培训。

2）不定期组织针对新员工的个人信息保护入职培训。

3）不定期组织定制化的个人信息保护培训。

12.4 培训方法：

1）举办专题讲座或培训班。

2）聘请有关专家进行讲课。

3）指派人员参加行业或者外单位的交流学习。

13.投诉举报

员工可通过 Foliday_compliance@fosun.com 举报任何违规行为。集团严格保护举报者不受打击和报复。

14.奖惩

14.1 对于在个人信息保护上提出切实可行的改进建议的，积极处理任何应急或风险事宜，或举报任何违法违规行为，为公司做出贡献或避免公司损失的员工，参照旅文集团奖惩制度进行奖励。

14.2 对于违反本制度的行为，将视情节严重和造成的后果，参照旅文集团奖惩制度进行处罚。如构成违法犯罪的，将交由行政机构和司法机构追究法律责任。

15.其他

15.1 本制度于 2022 年 8 月 23 日审批通过，并于 2022 年 8 月 29 日生效，于 2024 年 1 月 4 日更新发布。