白求恩公益基金会

白求恩公益基金会个人信息保护办法

会字〔2021〕第 08 号

第一章 总 则

第一条 为切实保护白求恩公益基金会(以下简称“基金会”)业务活动涉及的捐赠者和受助者等个人信息安全，维护其个人合法权益，根据《慈善法》《个人信息保护法》《基金会管理条例》《慈善组织信息公开办法》等法律、行政法规相关规定，制定本办法。

第二条 本办法所称的个人信息，是指基金会业务活动中收集、存储、使用、加工、传输、提供、公开、删除等涉及的信息。包括以电子或者其他方式记录的，能够单独或者与其他信息结合，识别特定自然人身份或反映特定自然人活动情况的各种信息，如姓名、出生日期、身份证号码、个人生物识别信息、住址、通信通讯、联系方式、通信记录和内容、账号密码、财产信息、信用信息、行踪轨迹、住宿信息、健康生理信息等。

第三条 本办法所称的个人敏感信息，是指一旦泄露、非法使用或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受损或遭遇歧视性对待等相关的个人信息，包括宗教信仰、生物识别信息、特定身份、财产信息、信用信息、行踪轨迹、健康生理信息等，以及不满十四周岁未成年人的个人信息。其中：

(一)财产信息包括：银行账号、存款信息(包括资金数量、

收支记录等)、交易和消费记录、流水记录等。

(二)健康生理信息包括:个人因生病医治活动等产生的相关记录，如病历、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、既往病史、诊治情况、家族病史、传染病史等，以及与个人身体健康状况相关的其他信息等。

(三)行踪轨迹包括:乘坐交通工具的票证购买信息和票证信息等。

(四)个人生物识别信息包括:个人基因、血液、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

第四条 基金会及各相关方(包括但不限于捐赠方、执行方、志愿者等）进行个人信息处理活动时，应遵循以下基本原则:

（一）目的明确原则:基金会及各相关方在个人信息处理活动中，应具有合法、正当、必要、明确的个人信息处理目的。

（二）选择同意原则:基金会及各相关方在个人信息处理活动中,必须向个人信息主体明确告知个人信息处理的目的、方式、范围、规则等，由个人信息主体通过书面（电子或纸质形式）声明或主动做出肯定性动作(主动勾选,主动点击“同意”“注册”“发送”“拨打”等）明确同意或授权。

（三）最少够用原则:除与个人信息主体另有约定外，基金会及各相关方应只处理满足目的所需的最少个人信息类型和数量，目的达成后，应及时根据约定删除个人信息。

（四）权责一致原则:基金会及各相关方在个人信息处理活动中造成个人信息主体合法权益损害的，应依法承担责任。

（五）公开透明原则：基金会及各相关方应当以明确、易懂和合理的方式，对处理个人信息的范围、目的、规则等进行公开，并接受外部监督。

（六）确保安全原则：基金会及各相关方应当具备与所面临的信息安全风险相匹配的风险处理能力，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。

第五条 基金会及各相关方不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

第二章 个人信息的收集

第六条 个人信息收集，是指基金会及相关方获得个人信息的行为，包括通过与个人信息主体交互或记录个人信息主体行为等主动采集、通过共享、搜集公开信息间接采集、由个人信息主体主动提供等方式。

第七条 基金会及各相关方收集个人信息时应满足合法性要求，不得从事下列行为：

（一）违反法律、行政法规要求。

（二）采用欺诈、诱骗、强迫手段。

（三）隐瞒产品或服务所具有的收集个人信息的功能。

（四）从非法渠道获取。

（五）收集法律、行政法规明令禁止收集的个人信息。

第八条 符合以下情形之一的，基金会及各相关方收集个人

信息无需征得个人信息主体的授权同意：

（一）与国家安全、国防安全直接相关的。

（二）与公共安全、公共卫生及重大公共利益直接相关的。

（三）紧急情况下为保护自然人的生命健康和财产安全所必需的。

（四）所收集的个人信息是个人信息主体向社会公众公开的。

（五）从合法公开披露的信息中收集个人信息的。

（六）根据个人信息主体要求签订和履行合同及合同性文件所必需的。

（七）法律、行政法规规定的其他情形。

第九条 基金会及各相关方收集个人敏感信息时，应取得个人信息主体的明确同意，并向个人信息主体告知个人信息的使用目的及拒绝提供带来的影响。

第十条 基金会及各相关方收集不满十八周岁的未成年人或年满十八周岁但无民事行为能力者的个人信息时，应征得其监护人的明确同意。

第三章 个人信息的保存

第十一条 基金会及各相关方对个人信息的保存应遵照法律、行政法规和基金会相关规章制度执行，并坚持保存期限最小化原则，个人信息使用目的达成后，应第一时间予以删除，使相关信息内容恢复不可被检索、访问和识别的状态。

第十二条 基金会收集个人信息后，应当立即进行去标识化

处理，并将去标识化后的数据与可用于恢复识别的数据分开存储，确保在后续的个人信息处理中不可被重新识别。

第十三条 基金会传输和存储个人敏感信息时，应采用加密等安全措施。

第十四条 在业务活动中断或结束后，基金会及各相关方应及时停止继续收集个人信息，并将相关中断或结束通知以逐一送达或公告的形式通知个人信息主体。

第十五条 基金会及各相关方，应当按照下列要求，做好个人信息删除工作：

（一）符合以下情形的，个人信息主体要求删除的，应及时删除个人信息：

1、违反法律、行政法规规定，收集、使用个人信息的。

2、违反与个人信息主体约定，收集、使用个人信息的。

3、约定的保存期限届满或处理目的已经实现。

4、法律、行政法规规定的其他情形。

（二）违反法律、行政法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，应立即停止共享、转让的行为，并通知第三方及时删除。

（三）违反法律、行政法规规定或与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，应立即停止公开披露的行为，并要求相关接收方删除相应的信息。

（四）业务活动任务停止或结束，业务活动各相关方按照本办法规定予以删除。

第四章 个人信息的使用

第十六条 基金会及各相关方应采取个人信息访问控制措施，以保障个人信息安全。个人信息访问控制措施包括：

（一）对被授权访问个人信息的内部数据操作人员，应按照最小授权的原则，使其只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。

（二）对个人信息的访问、修改、拷贝、下载等重要操作，应设置内部审批流程。

（三）对安全管理人员、数据操作人员、财务人员等不同角色进行分离设置。

（四）如确因工作需要，需授权特定人员超权限处理个人信息的，应由个人信息保护责任人进行审批，并记录在册。

第十七条 涉及通过界面展示个人信息的，基金会及各相关方应对需展示的个人信息采取去标识化处理，降低个人信息在展示环节的泄露风险，且应防止内部非授权人员及个人信息主体之外的其他人员获取个人信息。

第十八条 基金会及各相关方使用个人信息时，不得超出与收集个人信息时所声称的目的范围。因业务活动需要，确需超出范围使用个人信息的，应再次征得个人信息主体的明确同意。

第十九条 个人信息主体发现基金会及各相关方所持有的其个人信息有错误或不完整的，基金会及各相关方应根据个人信息主体要求进行更正或补充。

第二十条 基金会应建立个人信息主体行使权利的申请受理

和处理机制，由专人负责跟踪流程，并在合理的时间内对相关申诉进行响应。

第二十一条 基金会及各相关方应制定并及时更新个人信息安全事件应急预案，定期组织内部相关人员进行应急响应培训和演练，使其掌握应急处置策略和规程。

第二十二条 发生个人信息安全事件时，基金会及各相关方应及时将事件情况告知受影响的个人信息主体，并对事件处置结果及相关记录进行归档备查。

第五章 个人信息的委托处理、共享、转让、公开披露

第二十三条 委托处理个人信息时，应遵守以下要求：

（一）基金会作出的委托行为不得超出收集个人信息时个人信息主体授权或同意的范围。

（二）基金会应对委托行为进行个人信息安全评估，确保受托方具备相应的信息安全能力，以维护个人信息主体权益。

（三）基金会应通过合同等方式规定受委托方的责任和义务，对受托方进行监督，并要求受托方在委托关系解除时及时删除个人信息。

（四）基金会应准确记录和保存委托处理个人信息的情况及相关文件资料。

第二十四条 基金会及各相关方不得与任何第三方共享或者向任何第三方转让个人信息。

第二十五条 基金会及各相关方不得公开披露个人信息，基

金会履行法定义务或经法律授权或具备合理事由确需公开披露时，应充分重视风险，并根据《白求恩公益基金会基金会信息公开办法（修订）》进行披露。

第二十六条 基金会工作人员或各相关方违反本办法规定收集、保存、使用、共享、转让、公开披露以及非法买卖个人信息的，应承担由此产生的全部经济、行政和法律责任，基金会有权即时与其解除劳动合同或终止相关协议。

第六章 附 则

第二十七条 白求恩公益基金会拥有对本办法的最终解释权，并有权对本办法之条款进行修订。

第二十八条 本办法经2021年11月23日白求恩公益基金会第二届理事会第三次会议审议通过后施行。

主题词：个人信息 保护

白求恩公益基金会 2021 年 11 月制定(第一版)

（共印 份）