北京白求恩公益基金会

北京白求恩公益基金会个人信息保护办法

（修订版）

会字〔2022〕02号

第一章 总则

第一条 为切实保护北京白求恩公益基金会(以下简称为“基金会”)业务活动中涉及的捐赠人和受助人等个人信息安全，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、行政法规的有关规定和基金会章程，特制定本办法。

第二条 本办法所称的个人信息，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，不包括匿名化处理后的信息，包括自然人姓名、出生日期、身份证件号码，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。

第四条 本办法所称的个人信息处理，是指个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

第五条 基金会及各相关方（包括但不限于捐赠方、执行方、志愿者等服务提供者）进行个人信息处理活动，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，应当具有合法、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十分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，基金会及各相关方只处理满足个人信息主体授权同意的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，应依法承担相应的责任；

（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。

第六条 基金会业务活动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 个人信息的处理

第一节 一般规定

第七条 基金会及各相关方处理个人信息应当满足合法性要求，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处理个人信息的功能；

（四）从非法渠道获取；

（五）收集法律、行政法规明令禁止处理的个人信息。

第八条 符合以下情形之一，基金会及各相关方处理个人信息无需征得个人信息主体的授权同意：

（一）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；

（二）为履行法定职责或者法定义务所必需；

（三）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；

（四）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

（五）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

（六）法律、行政法规规定的其他情形。

第九条 基金会及各相关方处理个人敏感信息时，应取得个

人的单独同意、向个人告知处理敏感个人信息的必要性及对个人权益的影响。

第十条 基金会及各相关方处理不满 18 周岁的未成年人及限制民事行为能力人个人信息的，应征得其监护人的明示同意。

第二节 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期限，应当遵照法律、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，使相关信息内容保持不可被检索、访问、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个人的信息分开存储，确保在后续的个人信息处理中不重新识别个人。

去标识化，是指通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别特定自然人的过程。

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 在项目任务停止或结束后，基金会及业务活动各相关方应当及时停止继续收集个人信息的活动，将项目任务停止或结束的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 有下列情形之一的，基金会及各相关方应当主动删除个人信息，若未及时删除，个人信息主体要求删除的，应及时删除：

（一）处理目的已实现、无法实现或者为实现处理目的不再必要；

（二）业务活动任务停止或结束，或者保存期限已届满；

（三）个人撤回同意；

（四）违反法律、行政法规或者违反约定处理个人信息；

（五）法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，基金会及各相关方应当停止除存储和采取必要的安全保护措施之外的处理。

第三节 个人信息的使用

第十六条 基金会及业务活动各相关方应当采取个人信息访问控制措施，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)对个人信息包括批量修改、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、财务人员等的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；

(五)对个人敏感信息的访问、修改等行为，在对角色的权限控制基础上，根据业务流程的需求触发操作权。

第十七条 涉及通过界面展示个人信息的(如显示屏幕、纸面)，基金会及业务活动各相关方应对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。

在个人信息展示时，应当防止内部非授权人员及个人信息主体之外的其他人员未经授权获取个人信息。

第十八条 基金会及业务活动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目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。

将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，应对结果中所包含的个人信息进行去标识化处理。

第十九条 基金会及业务活动各相关方应向个人信息主体提供访问下列信息的方法：

(一)其所持有的关于该主体的个人信息或类型；

(二)上述个人信息的来源、所用于的目的；

(三)已经获得上述个人信息的第三方身份或类型。

个人信息主体提出访问非其主动提供的个人信息时，基金会或执行方可在综合考虑不响应请求可能对个人信息主体合法权益带来的风险和损害，以及技术可行性，实现请求的成本等因素后，做出是否响应的决定，并给出解释说明。

第二十条 个人信息主体发现基金会及业务活动各相关方所持有的该主体的个人信息有错误或不完整的，基金会及业务活动各相关方应为其提供请求更正或补充信息的方法。

第二十一条 个人信息主体撤回同意的，基金会及业务活动各相关方后续不得再处理相应的个人信息。

第二十二条 基金会应建立个人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，对申诉进行响应。

第四节 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) 基金会作出委托行为，应当与受托人通过合同的方式约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

（二）基金会作出委托行为，不得超出已征得个人信息主体授权同意的范围或遵守本办法关于收集个人信息时的授权同意规定的情形。

（三）基金会应对委托行为进行个人信息安全影响评估，确保受委托者具备相应的信息安全能力。

（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 受托者受基金会委托处理个人信息时，应遵守以下要求：

（一）受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；

（二）委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还基金会或者予以删除，不得保留；

（三）未经基金会同意，受托人不得转委托他人处理个人信息。

第二十五条 除本办法另有规定外，基金会及业务活动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。

第二十六条 基金会及业务活动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，并依据《北京白求恩公益基金会信息公开制度》实施。

第三章 个人信息的安全事件处置

第二十七条 基金会及业务活动各相关方，应按照下列要求，对个人信息安全事件进行应急处置和报告。

(一)制定个人信息安全事件应急预案；

(二)定期组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程；

(三)发生个人信息安全事件后，基金会及业务活动各相关方应根据应急响应预案进行以下处置：

1.记录事件内容，包括但不限于发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；

2.评估事件可能造成的影响，并采取必要措施控制事态，消除隐患；

3.按有关规定及时上报，报告内容包括但不限于涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；

4.对处置结果进行归档备查。

(四)根据相关法律、行政法规变化情况,以及事件处置情况,及时更新应急预案。

第二十八条 基金会及业务活动各相关方在发生安全事件时,应当及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时,应采取合理、有效的方式发布与公众有关的警示信息。

第二十九条 安全事件告知内容应包括但不限于安全事件的内容和影响、已采取和将要采取的处置措施、个人信息主体自主防范和降低风险的建议、针对个人信息主体提供的补救措施、安全事件处置负责人的联系方式等。

第四章 个人信息管理要求

第三十条 基金会及业务活动各相关方应当明确责任部门与人员:

(一)明确其法定代表人或主要负责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;

(二)明确个人信息保护工作机构,基金会信息保护工作部门为合规监察部;

(三)个人信息保护负责人和个人信息保护部门应履行的职责包括但不限于:

1.全面统筹实施基金会/企业内部的个人信息安全工作,对个人信息安全负直接责任;

2.应建立、维护和更新基金会/企业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；

3.开展个人信息安全影响评估；

4.组织开展个人信息安全培训。

第五章 法律责任

第三十一条 基金会工作人员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，应当承担基金会及个人信息主体因此产生的全部经济、行政和法律责任，基金会有权即时解除劳动合同。

第三十二条 基金会业务活动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，应当承担基金会及个人信息主体因此产生的全部经济、行政和法律责任，基金会有权立即终止相关协议。

第三十三条 本办法未尽事宜，按国家有关法律、法规和基金会章程的规定执行。

第六章 附则

第三十四条 本办法由基金会秘书处负责解释、修订。

第三十五条 本办法自基金会理事会通过后，公布之日起开始执行。原会字[2021]07号《北京白求恩公益基金会个人信息保护办法》即行废止。

主题词：个人信息 保护

北京白求恩公益基金会　　2021年3月制定（第一版）

2022年3月修订（第二版）