福建厦门福州泉州GB/T35273:2020个人信息安全管理体系认证证书申请办理代办机构费用

产品名称	福建厦门福州泉州GB/T35273:2020个人信息安全管理体系认证证书申请办理代办机构费用
公司名称	厦门文鹤企业管理有限公司
价格	48000.00/件
规格参数	品牌:厦门文鹤 型号:35273 产地:福建厦门
公司地址	厦门市集美区珩山街979号201室之一
联系电话	13459288341

产品详情

福建厦门福州泉州GB/T35273:2020个人信息安全管理体系认证证书申请办理代办机构费用

福建厦门福州泉州GB/T35273:2017认证，个人信息安全管理体系认证证书办理费用价格大约多少钱，需要哪些材料？需要什么条件？周期多久？需要多长时间？流程步骤怎么申请？

该标准代替GB/T 35273-2017《信息安全技术
个人信息安全规范》，与GB/T35273-2017相比，主要技术变化如下：

一是，增加了“ 多项业务功能的自主选择 ”、“ 用户画像的使用限制 ”、“ 个性化展示的使用 ”、“ 基于不同业务目所收集个人信息的汇聚融合 ”、“ 第三方接入管理 ”、“ 个人信息安全工程 ”、“ 个人信息处理活动记录 ”等内容；

二是修改了“ 征得授权同意的例外 ”、“ 个人信息主体注销账户 ”、“ 明确责任部门与人员 ”、附录C“ 实现个人信息主体自主意愿的方法 ”等内容。

《信息安全技术 个人信息安全规范》

范围

本标准规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动应遵循的原则和安全要求。

本标准适用于规范各类组织的个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。

规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2010 信息安全技术 术语

术语和定义

GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1 个人信息 personal information

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者反映特定自然人活动情况的各种信息。

注1：个人信息包括姓名、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、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：关于个人信息的判定方法和类型参见附录 A。

注3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，属于个人信息。

3.2 个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、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。

注2：关于个人敏感信息的判定方法和类型参见附录 B。

注3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，属于个人敏感信息。

3.3 个人信息主体 personal information subject 个人信息所标识或者关联的自然人。

3.4 个人信息控制者 personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。

3.5 收集 collect

获得个人信息的控制权的行为。

注1：包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人信息等行为。

注2：如果产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集。例如，离线导航软件在终端获取个人信息主体位置信息后，如果不回传至软件提供者，则不属于个人信息主体位置信息的收集。

3.6 明示同意 explicit consent

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。

注：肯定性动作包括个人信息主体主动勾选、主动点击“ 同意 ”“ 注册 ”“ 发送 ”“ 拨打 ”、主动填写或提供等。

3.7 授权同意 consent

个人信息主体对其个人信息进行特定处理作出明确授权的行为。

注：包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权（如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。

3.8 用户画像 user profiling 通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特

定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

3.9 个人信息安全影响评估 personal information security impact assessment

针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造

成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。

3.10 删除 delete

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

3.11 公开披露 public disclosure

向社会或不特定人群发布信息的行为。

3.12 转让 transfer of control

将个人信息控制权由一个控制者向另一个控制者转移的过程。

3.13 共享 sharing

个人信息控制者向其他控制者提供个人信息，且双方分别对个人信息拥有独立控制权的过程。

3.14 匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过

程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

3. 去标识化 de-identification

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，无法识别或者关联个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

3.16 个性化展示 personalized display

基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。

3.17 业务功能 business function

满足个人信息主体的具体使用需求的服务类型。

注：如地图导航、网络约车、即时通讯、网络社区、网络支付、新闻资讯、网上购物、快递配送、交通票务等。

4. 个人信息安全基本原则

个人信息控制者开展个人信息处理活动应遵循合法、正当、必要的原则，具体包括：a) 权责一致——采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任；

目的明确——具有明确、清晰、具体的个人信息处理目的；

选择同意——向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意；

小必要——只处理满足个人信息主体授权同意的目的所需的少个人信息类型和数量。目的达成后，应及时删除个人信息；

公开透明——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督；

确保安全——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；

主体参与——向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。