

个人信息保护政策

发布日期：2021年【 12 】月【 16 】日

生效日期：2021年【 12 】月【 16 】日

前言

感谢您对深圳市电子商务安全证书管理有限公司（以下简称“SZCA”或“我们”）的信任。我们深刻认识并理解个人信息对您的重要意义，并通过技术、政策、制度、流程等多项措施加强个人信息安全及保护。《个人信息保护政策》（以下简称“本政策”）将向您说明我们如何收集、存储、使用及对外提供、转让您的个人信息，并说明您所享有的访问、更正、删除、改变授权同意范围、账户注销、获取个人信息副本等权利，主要要点如下：

1、为了向您提供产品和服务所需，SZCA按照合法、正当、必要和诚信的原则开展个人信息处理活动，具体包括：权责一致原则、目的明确原则、选择同意原则、最小必要原则、确保安全原则、主体参与原则、公开透明原则；

2、SZCA将结合具体的产品和服务，向您逐一说明所收集的信息类型与用途；

3、为向您提供某些产品与/或服务之目的，我们可能需要将您的个人信息向第三方提供并由其处理。我们将在评估并确认第三方满足收集个人信息的合法、正当、必要性之后，向第三方提供您的个人信息，并要求其按照法律、法规的规定及国家标准，对您的个人信息采取严格的保护措施。

4、将您的个人信息向第三方提供之前，我们将通过弹窗、文本确认等方式征得您的单独同意，但依法无需获得授权同意的场景除外。因向您提供产品与/或服务所需，我们拟超出原本的获得的授权同意范围处理您的个人信息前，将会再次征得您的同意。

5、您可以通过本政策所列的方式实现您对个人信息的有关权利，您也可以在权利受到侵害的情形下向我们进行举报。

6、本政策适用于用户向SZCA申请SZCA的电子认证、数字证书、电子签名等所有相关产品与/或服务，具体SZCA自主开发运营的业务平台包括但不限于证聚（含网站、APP、微信小程序）、掌信签（含网站、APP、微信小程序、及SDK）、云签（含网站及微信小程序）、数必安（Themis）、医疗云签微信小程序等。SZCA成立于2000年，注册地址为：深圳市南山区高新中二路深圳软件园一期8栋301。如果您有任何疑问、意见或建议，请通过以下联

系方式与SZCA联系：

- 1) 电子邮件： kfzz@szca.com
- 2) 电 话： 0755-26588399/4001123838
- 3) 传 真： 0755-8615 6366
- 4) 电话： 0755-26588399

第一部分 定义

1. 业务平台：包括域名为【szca.com】的网页及名称包括或含有【深圳 CA】、【掌信签】、【云签】、【医疗云签】、【证聚】、【数必安】或【Themis】的【APP、微信小程序、公众号、H5 页面】等 SZCA 运营的自有客户端。
2. 个人信息：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. 有权的国家机关、企事业单位或其他组织：拥有合法资质的数据库运营机构，包括公安部、银联、国家工商部门、运营商、征信机构，及其代理商、关联公司等。
4. 关联公司：控制某一实体、受某一实体控制或与某一实体处于共同控制下的公司、机构。“控制”指通过所有权、有投票权的股权、合同、实际运营关联或其他被依法认定的方式直接或间接拥有影响对被控制对象管理/经营的能力。
5. 敏感个人信息：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，以及儿童的个人信息。
6. 儿童：不满十四周岁的未成年人。

第二部分 个人信息保护政策

请您在使用 SZCA 的产品与/或服务或业务平台前，请您仔细阅读并了解《XXX 个人信息保护政策》，特别是加粗字体的条款，您应当重点阅读，在充分理解后开始使用业务平台。本政策将帮助您了解详细内容：

- 一、我们如何收集和使用您的个人信息
- 二、我们如何保存您的个人信息

三、我们如何使用 COOKIE 和同类技术

四、我们如何委托处理、提供、转移、公开披露您的个人信息

五、我们如何保护您的个人信息

六、您的权利

七、我们如何处理与保护儿童的个人信息

八、本政策如何更新

九、如何联系我们

一、我们如何收集和使用您的个人信息

根据相关法律、法规和监管要求，遵循合法、正当、必要的原则，我们基于以下目的，收集和使用您的个人信息。该等个人信息因您使用业务平台具体产品与/或服务而向我们主动提供，或因您使用我们的产品与/或服务或业务平台而由我们收集，或由我们向第三方获取。**无论哪种方式，原则上都在获取您的同意后进行，除非法律另有规定或者基于保护您或者其他人的重要利益。**您可以选择不提供，或仅提供部分的信息，但这可能导致无法使用，或无法正常使用全部的产品与/或服务。

1. 用户注册及登录

1.1 账户实名制：您注册我们的业务平台账户时，根据国家互联网实名制、网络信息安全管理的要求，SZCA 将收集您的**姓名、手机号码、电子邮箱**。SZCA 将收集您的这些信息并向有权的国家机关、企事业单位或其他组织进行验证，并获取验证结果。若您不提供这类信息，将无法登陆业务平台或无法正常使用产品和服务。

1.2 账户安全：为了确保账号的安全性，识别账号使用异常，在您登录、使用包括但不限于证聚、云签或掌信签等 App、网页、小程序的过程中，SZCA 可能需要收集您的**常用设备信息，包括唯一设备识别码、IP 地址、设备 MAC 地址、操作行为信息**，以便对您身份以及行为安全性进行核实、管理，例如：在您进行特定线上操作时，通过比对您的常用设备信息确认相关操作行为是否存在异常。

2. 证书申请、审核、使用与生命周期管理

2.1 证书办理的实名认证

为申请 SZCA 数字证书有关产品与/或服务，包括数字证书新办、续期、变更、密钥更新业务等，根据数字证书产品应用场景及项目业务应用安全需求，您可以通过以下方式提交以下个人信息。

通过 SZCA（含各自营受理点、营业部、分公司等 SZCA 附属机构）、或业务平台办理 SZCA 产品与/或服务的，您同意填写或提交**本人的姓名、身份证号、手机号码、居住地址、电子邮箱、身份证影印件、本人手持身份证影印件、本人手持办证资料（如申请表、服务协议）等的影印件**。在您借助身份认证设备机具办理业务的，您需授权认证设备采集、识别**您的姓名、手机号码、身份证件信息（含姓名、身份证号、身份证有效期、居住地址）**，授权设备摄像头拍摄**您的人脸影像信息、或设备指纹采集器件采集您的指纹信息**。在您通过移动设备自助使用本功能时，我们会请求您授权**【相机权限】或【摄像头权限】**用于收集您**身份证影印件、面部特征信息、银行卡信息（银行卡开户人姓名、身份证号、卡号、手机号）等的个人信息**。

当您与 SZCA 有商业合作关系的合作机构发生交易，使用合作机构的产品与/或服务，且同时需要应用 SZCA 的产品与/或服务时，合作机构在征得您的授权同意后，出于为您申请办理享用 SZCA 产品与/或服务的目的，将向 SZCA 传输、提供合作机构采集的 SZCA 业务办理所必须的上述个人信息。SZCA 在受理审核业务申请时，除审核验证您的身份信息等信息之外，也将采取适当措施保障信息提供有得到您的合法授权，要求合作机构承诺采集并提供您的个人信息给 SZCA 行为的合法合规。

SZCA 签发数字证书及为您提供其他证书管理服务，需要对收集的您的包括但不限于身份信息在内的各种个人信息进行验证，包括验证身份证明材料的真实性、准确性及完整性，及鉴别申请人身份的真实性。为实现实名认证的目的，您同意我们可以自行或委托第三方向依法有权保存您个人身份信息的国家机关、企事业单位或其他组织提供、查询、核对您的身份信息。

SZCA 将您提交的申请认证所需的前述个人信息，及从第三方处收集验证的信息，统一汇集，进行比较甄别，在确认您身份真实性的基础上，据此作出数字证书签发等业务办理决定。SZCA 将为您签发包含您的姓名、地址等真实个人信息在内的数字证书。特定类型数字证书，如场景证书或其他用户定制的证书，也将写入您的设备信息或其他您需要载入用户证书的信息。**若您不提供这类信息（含指纹、人脸信息），将无法申请、使用 SZCA 的数字证书、电子签署等产品和服务。**

2.2 证书领取与使用的安全控制

为了保障数字证书使用的安全性，确保证书由您本人领取、保管或控制使用，SZCA 将通过密码验证、短信 OTP 验证、人脸识别活体验证或指纹验证、金融打款验证，或需要您拍摄手持数字证书 UKEY 或数字证书 UKEY 签收单等其中一种或多种方式，核验您的身份，确认证书签署、加密、登录等使用行为均由您本人进行，证书操作指令由您本人发出。为进行证书领取、使用的实名身份验证，您同意我们可以通过您自行填写、通过移动设备采集、或通过向保存您有关信息政府机构、企事业单位或其他组织查询并获取您的**手机号码、银行卡号、人脸面部影像信息、指纹特征信息**，进行相关的比对核验。

2.3 证书生命周期管理服务的实名制

在您申请办理数字证书撤销、挂起、冻结、密钥恢复、数字证书资料调取、或证书证明开具等业务时，SZCA 将核实您的身份，确保为您本人申请，方会为您办理业务，以保障用户数字证书的安全使用。在您使用本项产品与/或服务或功能时，SZCA 收集和使用您的个人信息，按照上述 2.1 的规定进行。

您提供的上述信息，将在您使用本项产品与/或服务期间持续授权我们使用。在您停止使用我们的服务或产品时，我们将停止使用您的该项信息，并在按法律保存法定期间后予以删除。关于保存期限，详见本政策“五、信息的存储”。

3. 合作机构业务所需的防欺诈与风险控制

在您使用 SZCA 的合作机构的产品与/或服务时，当该合作机构采购应用 SZCA 的身份认证服务对您进行实名认证，以进行欺诈识别筛查与业务风险控制的，您同意 SZCA 通过合作机构**收集您的姓名、身份证号码、手机号码、身份证信息（含身份证号、姓名、居住地、身份证有效期），银行卡信息（银行卡开户人姓名、身份证号、卡号、手机号），面部特征、指纹信息等**。SZCA 会对该等合作机构提供的信息来源合法性作出要求，并在条件允许情况下，与合作机构签订身份鉴别责任划分的协议，确保从合作机构获取的信息的真实性、有效性。**但请您理解，基于现有法律法规的规定和权限限制，我们无法保证合作机构网站的运营会完全按照 SZCA 的要求采取措施，您应当仔细阅读他们的服务协议及个人信息保护政策。**

基于合作机构的业务需要，SZCA 在确保合作机构得到用户合法授权的情况下，对合作机构提供的您的前述个人信息，提供给合法存有您信息的第三方机构（政府机关、企事

业单位或其他组织) 核实个人信息的真实性, 以保障用户身份的真实性, 防范合作机构业务过程中的欺诈或业务虚假行为。

4.产品与/或服务质量改善: 在前述之外, 为优化服务质量, 提升用户体验, SZCA 可能需要收集您产品与/或服务使用过程中产生的信息, 并将该等信息储存为日志信息, 进行故障分析与问题诊断修复, 并采取必要的记录、审计、分析、处置相关措施。日志信息包括: 如您的移动设备、软件、网页浏览器或用于接入 SZCA 服务的其他程序所提供的配置信息 (如计算机、浏览器、软件的类型、使用的语言、访问日期和时间、及访问的网页记录; 终端设备的操作系统、电信运营商等)、您的 IP 地址和移动设备所用的版本和设备识别码。

5.服务通知推送: 您知悉并同意, 对于您在使用我们业务平台过程中提供的您的一种或多种联系方式 (如: 联系电话、电子邮箱), 我们在运营中可能会向其中的一种或多种发送多类通知, 用于业务服务消息告知 (含业务受理通知、证书应用安全通知)、身份验证、安全验证、用户使用体验调研等用途。必要时, 或在您选择个性化服务时, 也将推送证书续期、证书密钥更新等提醒通知。我们可能会将通过活动获得的您的相关信息, 用于研发和改进产品和服务、综合统计、数据分析或加工等或经您授权同意的其他用途。

6.其他个人信息处理规则

6.1 在收集您的个人信息后, 我们会立即通过技术手段对数据进行去标识化处理, 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内部权限管理, 去标识化处理的个人信息将无法用于识别您的身份。请您了解, 在不对外提供您个人信息的前提下, 我们有权对数据库中去标识化的数据进行统计、分析, 为我们的商业决策提供产品与/或服务支持, 以及改进我们的产品与服务。

6.2 请您注意, 您在使用我们的产品与/或服务时所提供的所有个人信息, 除非您已经停止使用我们的产品与/或服务, 并向我们提出撤回对您个人信息的授权同意, 否则我们有权持续使用有关的个人信息。

6.3 我们会对我们的产品与/或服务使用情况进行统计, 并可能会与公众或第三方共享这些统计信息, 以展示我们的产品与/服务的整体使用趋势。但这些统计信息不包含您的任何身份识别信息。

6.4 当我们业务平台展示您的个人信息时, 我们会采用包括内容替换、假名处理方式对您的信息进行脱敏, 以保护您的信息安全。

6.5 当我们要将您的个人信息用于本政策未载明的其它用途时, 或基于特定目的收集而来的信息用于其他目的时, 我们会通过弹窗、文本确认或其他合理的方式征求您的同

意。

6.6 征得授权同意的例外：根据法律法规及国家机关的监管要求，在以下情形中，我们的业务平台收集、使用个人信息无需征得您的授权同意：

- 与国家安全、国防安全有关的；
- 与公共安全、公共卫生、重大公共利益有关的；
- 与犯罪侦查、起诉、审判和判决执行等有关的；
- 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；
- 所收集的个人信息是个人信息主体或监护人自行向社会公众公开的；
- 从合法公开披露的信息中收集的您的个人信息的，如合法的新闻报道、政府信息公开等渠道；
- 根据您的要求签订合同所必需的；
- 用于维护所提供的产品与/或服务的安全稳定运行所必需的，例如发现、处置产品与/或服务的故障；
- 法律法规规定的其他情形。

二、我们如何保存您的个人信息

1. 存储地点与存储期限

您的个人信息将存储于中华人民共和国境内。在您申请数字证书及使用其相关服务时，SZCA 对于为您提供认证服务所收集、产生的您的相关个人信息将进行保存，且保存时间在提供产品与/或服务期间将一直持续；并且按照《电子签名法》等的规定，在订购产品与/或服务结束证书注销后，因调查取证、归档备份等 SZCA 仍将保存上述信息至少 5 年，涉及应用到政务领域、系统的证书的，将至少保存至证书失效后 10 年，法律法规另有规定的除外。SZCA 仅在本政策所述目的所必需期间和法律法规要求的时限内保留您的个人信息。对于为其他业务目的收集使用的信息，保存期限为您停止使用业务平台产品及服务，且**您在通过业务平台与我们的合作机构的业务全部结束后**五年。超过保存期限，SZCA 将删除您的个人信息。但在下列情况下，我们可能会根据有关法律法规的要求，调整个人信息存储时间：

- 为遵守适用的法律法规的有关规定；
- 为遵守法院判决、裁定或其他法律程序的规定；

- 为遵守相关政府机关或法定授权组织的要求；
- 为维护社会公共利益，保护业务平台其他用户的合法权益所必须。

2. 跨境传输

若有提供产品与/或服务的必要，在获得您的单独同意后，您的个人信息可能会被转移到您使用产品或服务所在国家/地区的境外管辖区。在获得您的单独同意时，我们会通过弹窗、文本确认或其他合理的方式向您明示告知接收，以及其处理您个人信息的目的、方式和种类。**具体的单独同意形式，以具体产品与/或服务的提供页面或书面材料为准。**

以上境外管辖区可能设有不同的数据保护法律，甚至未设立相关法律。在此类情况下，我们会确保您的个人信息得到在中华人民共和国境内足够同等的保护。例如，我们会请求您对跨境转移您的个人信息提供单独同意，或者在跨境数据转移之前实施个人信息的匿名化举措。

3. 停止存储

如果我们终止服务或运营，我们会至少提前九十日向您通知，并在终止服务或运营后对您的个人信息进行删除或匿名化处理。

三、我们如何使用 COOKIE 和同类技术

1、为使您获得更轻松访问的体验，您访问业务平台或使用业务平台提供的服务时，业务平台可能会通过小型数据文件识别您的身份，这么做是帮您省去重复输入相关信息的步骤，或者帮助判断账户安全。这些数据文件可能是Cookie，Flash Cookie，或您的浏览器或关联应用程序提供的其他本地存储（统称“Cookie”）。

2、请您理解，我们的某些服务只能通过使用“Cookie”才可得到实现。如果您的浏览器或浏览器附加服务允许，您可以修改对Cookie的接受程度或者拒绝业务平台的Cookie，但这一举动在某些情况下可能会影响您安全访问业务平台和使用业务平台提供的服务。

3、网页上常会包含一些电子图象（称为“单像素” GIF文件或“网络Beacon”），使用网络Beacon可以帮助网站计算浏览网页的您或访问某些Cookie，业务平台会通过网络Beacon收集您浏览网页活动的信息，例如您访问的页面地址、您先前访问的援引页面的位址、您停留在页面的时间、您的浏览环境以及显示设定等。

四、我们如何委托处理、提供、转移、公开披露您的个人信息

1. 委托处理

为向您提供【第一条第1.1项、第2项、第3项】所述功能模块及对应的服务，我们聘请具备专业技术能力的第三方供应商提供，并委托其处理相关个人信息。

对SZCA委托处理个人信息的公司、组织和个人，我们会与其签署严格的委托处理协议，并对其进行个人信息安全影响评估，要求他们按照本政策以及其他任何相关的法律法规的要求来处理个人信息。同时，我们会记录和存储受委托者处理个人信息的情况。一旦我们得知或者发现受委托者未按照委托要求处理个人信息，或未能有效履行个人信息安全保护责任的，将立即要求受委托者停止相关行为，且采取或要求受委托者采取有效补救措施控制或消除您的个人信息面临的安全风险。

委托关系未生效、无效或被撤销、终止时，我们将终止与受委托者的业务关系，并要求受委托者及时返还或删除从业务平台获得的您的个人信息(包括但不限于因委托处理获取的原始的个人信息或副本、摘要等)，不得擅自保留。未经您的授权同意，我们禁止受委托者转委托他人处理您的个人信息。

2. 提供

(1) 我们不会向SZCA以外的任何公司、组织和个人提供您的个人信息，但以下情况除外：

- **事先获得您明确的同意或授权；**
- 根据适用的法律法规、法律程序的要求、强制性的行政或司法要求所必须的情况下进行提供；
- 在法律法规允许的范围内，为维护我们、平安集团及关联公司或合作伙伴、您或其他用户或社会公众利益、财产或安全免遭损害而有必要提供；
- **只有提供您的信息并经您同意，才能实现业务平台的产品与/或服务的核心功能或提供您需要的服务；**
- 应您需求为您处理您与他人的纠纷或争议；
- **符合与您签署的相关协议（包括在线签署的电子协议以及相应的平台规则）或其他法律文件约定所提供；**
- 基于符合法律法规的社会公共利益而使用。

(2) 我们只会对外提供必要的个人信息，且受本政策中所声明目的之约束。个人信息

的接收方如要改变个人信息处理目的，将再次征求您的授权同意。

(3) 为了保障数据在第三方安全可控，我们事先将开展个人信息安全影响评估，并依评估结果采取有效的个人信息保护措施，例如，通过合同约定数据接收方的个人信息保护责任。我们要求数据接收方用于存放您的个人信息的系统满足信息安全等级保护三级要求。在敏感个人信息使用上，我们要求第三方采用数据脱敏和加密技术，从而更好地保护用户数据。我们发现数据接收方违反法律法规要求或双方约定处理个人信息的，将立即要求数据接收方停止相关行为，且采取或要求数据接收方采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除您的个人信息面临的安全风险；必要时，我们将解除与数据接收方的业务关系，并要求数据接收方及时删除从我们处获得的您的个人信息。

3.转移

我们不会将您的个人信息转移给任何公司、组织和个人，但以下情形除外：

- **事先获得您明确的同意或授权；**
- 在涉及合并、收购或破产清算时，如涉及到个人信息，我们会要求新的持有您个人信息的公司、组织继续受本政策的约束，否则我们将要求该公司、组织重新向您依法征得授权同意；
- 根据适用的法律法规、法律程序的要求、强制性的行政或司法要求所必须进行转移。

我们会采取在其它服务器备份、在传输和存储过程中对您数据和鉴别信息进行加密等安全措施，最大程度确保您的个人信息不丢失，不被滥用和变造。**但同时也请您理解，在信息网络上不存在“完善的安全措施”。金融壹账通无法承诺您数据及信息的完全安全。**

4.公开披露

我们仅会在以下情形下，公开披露您的个人信息：

- **事先获得您明确的同意或授权；**
- 根据适用的法律法规、法律程序的要求、强制性的行政或司法要求，我们可能会公开披露您的个人信息。

我们将对所有的请求进行慎重的审查和事先的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，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，以确保其具备合法依据，且披露的个人信息范围仅限于执法部门因特定调查目的且有合法权利获取的数据。在法律法规许可的前提下，我们披露的数据和文件均在加密密钥的保护之下。

5. 第三方 SDK 服务商

为保障【XXX】平台的稳定运行和功能实现，在某些特定使用场景下，【XXX】平台会嵌入具有相应资质及能力的第三方服务商提供的软件服务工具包（以下简称“SDK”）或其他类似应用程序。我们会对业务合作伙伴获取个人信息的 SDK 及其中的应用程序接口（以下简称“API”）进行严格的安全检测，令其按照第三方服务商披露的个人信息保护政策及类似文本来处理您的个人信息。我们接入的第三方 SDK 服务商的名称、收集的您的个人信息的类型与目的如下：

第三方 SDK 名称	第三方服务商	收集的信息字段	个保政策链接	业务场景/使用目的

但请您理解，基于现有法律法规的规定和权限限制，我们无法保证第三方服务商的运营会完全按照我们的个人信息保护政策与要求，您应当仔细阅读该等第三方的服务协议及个人信息保护政策。

五、我们如何保护您的个人信息

SZCA 将尽合理努力保护其收集获取的用户个人信息。为防止用户个人信息在未经授权的情况下被非法访问、泄露、篡改、传输、遗失、毁损、滥用或编造、处理或使用，SZCA 已经并将继续采取以下措施保护你的个人信息：

1.人员安全

SZCA 高度重视信息安全保障工作，对于认证岗位的设置实行可信角色制。且对于拟招聘任用的人员，在正式上岗前，都统一进行员工背景调查，尤其是对于可信角色等关键岗位的任职员工，将进行严格的安全意识和能力的考察。此背景调查一般每 3 年开展一次，确保员工遵循信息安全方面的规范。并且在任用时与其签订保密协议，禁止员工在劳动关系期间及合同期满 2 年内非法泄露工作过程中知悉的用户个人信息。

SZCA 注重员工信息安全意识与能力的培养，定期开展信息安全与隐私保护相关技术及法律等方面的培训，结合信息安全知识的考核，提高员工有关信息安全的认识。

SZCA 设置有专门的负责信息安全的岗位——安全管理员，并为其配备专门的信息安全管理人员，监督认证服务过程中用户信息的处理与传输，确保用户个人信息的合法收集、使用与披露。

2.技术安全措施

SZCA 在数据安全保障方面，执行符合行业标准的安全措施与技术手段、程序，防止数据遭到未经授权访问、公开披露、使用、修改、损坏或丢失。SZCA 会采取一切合理可行的措施，保护您的个人信息。例如，网络服务采取传输层安全协议等加密技术，通过 https 等方式提供浏览服务，确保用户数据在传输过程中的安全。采取加密技术对用户个人信息进行加密保存，并通过隔离技术进行隔离。在个人信息使用时，例如个人信息展示、个人信息关联计算，SZCA 会采用包括内容替换、SHA256 在内多种数据脱敏技术增强个人信息在使用中安全性。我们采用严格的数据访问权限控制和多重身份认证技术保护个人信息，避免数据被违规使用，采用代码安全自动检查、数据访问日志分析技术进行个人信息安全审计。

3.访问控制

SZCA 设立严格的数据访问制度，采用严格的数据访问权限控制和多重身份认证技术保护个人信息，避免数据被违规使用。对可能接触到您信息的员工，SZCA 采取最小够用授权原则，能够访问、控制您信息的员工限定在工作职责需要有必要知悉您信息的直接相关的工作人员，及高级管理人员。且其访问、改动信息的操作，是要进行身份的识别与验证，且需接受视频监控。且要求上述员工履行保密和安全义务。如其未能履行安全和保密义务，将与其解除劳动合同关系，且保留追究其法律责任的权利。

此外，SZCA 采取专门的数据和技术安全审计，设立日志审计和行为审计多项措施。定期对用户信息等数据访问记录进行审计检查，保证信息的访问、传播与扩散，是按照 CPS 规定的程序及方式进行的，控制在业务必需及可支配的范围内。

4.加密传输与存储

通过采取加密技术对用户个人信息进行加密保存，并通过隔离技术进行隔离。

5.脱敏显示

在个人信息使用时，例如个人信息展示、个人信息关联计算，SZCA 会采用包括加密脱敏等多种数据脱敏技术增强个人信息在使用中安全性。SZCA 将对您服务界面中您的“个人中心”的手机号码、身份证件、护照、港澳通行证等个人信息采取隐私处理措施，避免您设备被不当使用时所造成的信息泄露与丢失。

6.数据安全管理机制

通过信息接触者保密协议、监控和审计机制来对数据进行全面安全控制。SZCA 系统通过了公安部安全等级保护三级认证，同时还获得了 ISO27000 认证。

7.应急处理措施

SZCA 制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，在发生危害网络安全的事件时，SZCA 会立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。并且将定期组织负责信息安全的重要成员进行安全预案演练。

8.安全事件处置

在不幸发生个人信息安全事件后，我们将按照法律法规的要求，及时向您告知：安全事件的基本情况、可能的影响、我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。我们将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您，难以逐一告知个人信息主体时，我们会采取合理、有效的方式发布公告。同时，我们会严格按照有关法律法规及监管部门要求，主动上报个人信息安全事件的处置情况。

9. 如果您对我们的个人信息保护有任何疑问，可通过本政策中约定的联系方式联系我们。如您发现自己的个人信息存在安全隐患，尤其是您的账户及密码发生泄露，请您立即通过本政策【九、如何联系我们】中披露的联系方式联络我们，以便与我们采取相应措施。

六、您的权利

按照我国的法律、法规及标准，SZCA 保障您对自己的个人信息行使以下权利：

1.访问、更正您的个人信息

您有权访问您的个人信息，法律法规规定的例外情况除外。若您发现我们的业务平台处理的关于您的个人信息有错误时，您有权要求我们作出更正。您可以通过以下方式自行访问或更正我们的业务平台留存的您的个人信息：

登录业务平台 APP，点击“个人中心”、“我的”、“我的账户”“账户管理”或其他类似界面，对您的姓名、身份证号或数字证书数据进行查询访问、更正，其中身份证件号码信息将采取脱敏化方式予以显示。

如果您无法通过上述方式访问这些个人信息，您可以通过拨打【4001123838】联系，或发送电子邮件至【kfzz@szca.com】，我们将在 15 个工作日内回复您的请求。对于您在使用我们业务平台的产品或服务过程中产生的其他个人信息，在核实您的真实身份的前提下，我们会以合理方式向您提供访问与/或更正的路径。

2.删除您的个人信息

在以下情形中，您可以向 SZCA 提出删除个人信息的请求：

- 如果我们处理个人信息的行为违反法律法规；
- 如果我们收集、使用您的个人信息，却未征得您的同意；
- 如果我们处理个人信息的行为违反了与您的约定；
- 如果我们不再为您提供产品或服务。

如果您需申请删除您的个人信息，您可以通过拨打【4001123838】联系，或发送电子邮件至【kfzz@szca.com】，我们将在 15 个工作日内回复您的请求，法律法规另有规定的除外。

若我们决定响应您的删除请求，我们还将同时通知从业务平台获得您的个人信息的第三方实体，要求其及时删除，除非法律法规另有规定，或这些实体获得您的独立授权。当您从我们的服务中删除您的个人信息后，出于安全考虑，我们可能不会立即在备份系统中删除相应的信息，但会在备份更新时删除这些信息。

3.改变您授权同意的范围

我们的业务平台的产品与服务需要一些基本的个人信息才能得以完成，在您与我们业务平台的业务以及通过我们的业务平台与我们的合作机构发生的业务全部结束前，您无法撤回针对必要个人信息处理的授权同意。对于可选的个人信息类型的收集和使用，您可以随时给予或收回您的授权同意。

您可以通过以下方式自行操作授权同意的撤回：

- 通过删除个人信息、关闭设备权限或功能、在【XXX】平台中进行“个人中心”、“我的”、“我的账户”“账户管理”或其他类似等界面设置，改变您授权我们继续收集个人信息的范围、或撤回您的授权。
- 通过注销账户的方式，撤回我们继续收集与使用您个人信息的全部授权。

如果您无法通过上述方式实现撤回授权同意的请求，您可以通过拨打【4001123838】联系，或发送电子邮件至【kfzz@szca.com】，我们将在 15 个工作日内回复您的请求。

当您撤回授权同意后，我们将不再处理相应的个人信息。但您收回同意的决定，不会影响此前基于您的授权而开展的个人信息处理。

4.注销账户

您可以通过以下方式自行操作：您可以通过访问“个人中心”、“我的”、“我的账户”“账户管理”界面或其他类似界面，申请注销证书或停止服务。

如果您无法通过该界面注销您的个人信息相关服务，可以通过拨打【4001123838】联系，或发送电子邮件至【kfzz@szca.com】联系我们提交申请，我们将在 15 个工作日内核实您的真实身份并处理。在注销账户之后，我们将停止为您提供一切产品或服务，并依据您的要求，在符合法律法规规定的前提下，删除您的个人信息。

5.获取个人信息副本

您有权获取您的个人信息副本，您可以通过以下方式自行操作：本人携带身份证至 SZCA 现场，或通过邮寄本人申请文件，拨打【4001123838】联系，或发送电子邮件至【kfzz@szca.com】联系我们提交申请，SZCA 将以邮寄、电子邮件、现场复印等方式提供副本。

6.其他须知

为保障安全，在通过邮件请求您的个人信息权利时，您可能需要根据我们提供的模板提供书面请求；在通过电话请求时，您允许我们对您的请求进行核实，并全程录音。但无论以何种方式，您承诺按照我们的要求提供您的身份信息用于身份核实，在此基础上，我们将会处理您的请求，并在 15 个工作日内作出答复。

对于您合理的请求，我们原则上不收取费用，但对多次重复、超出合理限度的请求，我们将视情收取一定成本费用。对于那些无端重复、需要过多技术手段（例如，需要开发新系统或从根本上改变现行惯例）、给他人合法权益带来风险或者非常不切实际（例如，涉及备份磁带上存放的信息）的请求，我们可能会予以拒绝。

七、我们如何处理与保护儿童的个人信息

我们的产品、服务及网站主要面向成年人。如果没有父母或监护人的同意，包括儿童在内的未成年人不得创建自己的业务平台账户。对于经父母同意而收集儿童个人信息的情况，我们只会在受到法律允许、父母或监护人明确同意或者保护儿童所必要的情况下使用此信息。

尽管当地法律和习俗对儿童的定义不同，但我们将不满 14 周岁的任何人均视为儿童。如果我们发现自己在未事先获得可证实的父母同意的情况下收集了儿童的个人信息，则会尽快删除相关数据。

八、本政策如何更新

本政策可能变更，未经您明确同意，我们不会削减您按照本政策所应享有的权利。

我们会在我们的业务平台页面上发布对本政策所做的任何变更。对于重大变更，我们还会提供更为显著的通知（包括站内信，或通过电子邮件发送通知，说明个人信息保护政策的具体变更内容）。

本政策所指的重大变更包括但不限于：

- 我们的服务模式发生重大变化。如处理个人信息的目的、处理的个人信息类型、个人信息的使用方式等；

- 我们在所有权结构、组织架构等方面发生重大变化。如业务调整、破产并购等引起的所有者变更等；
- 个人信息提供、转移、转让或公开披露的主要对象发生变化；
- 您参与个人信息处理方面的权利及其行使方式发生重大变化；
- 我们负责处理个人信息安全的责任部门、联络方式及投诉渠道发生变化时；
- 个人信息安全影响评估报告表明存在高风险时。

我们还会将本政策的 3 年以内的过往版本存档，供您查阅。访问地址：

<https://www.szca.com>，访问路径：首页-客户服务-电子认证法律法规。

九、如何联系我们

1、如果您有任何疑问、意见或建议，请通过以下方式与我们联系：

公司名称：深圳市电子商务安全证书管理有限公司

电话：0755-26588399/4001123838

传真：0755-8615 6366

电子邮件：kfzz@szca.com

邮寄地址：深圳市南山区高新中二道深圳软件园 8 栋 301 室[518057]

2、一般情况下，我们将在 15 个工作日内回复您的诉求。如果您对我们的回复不满意，特别您认为我们的个人信息处理行为损害了您的合法权益，您还可以通过以下外部途径寻求解决方案：联系负责个人信息保护相关投诉的有关行业协会、主管部门，或者依据适用的法律向具有管辖权的法院提起诉讼。