

# 个人信息保护政策

更新日期：2025 年 05 月 12 日

生效日期：2025 年 05 月 12 日

欢迎您使用湖北省数字证书认证管理中心有限公司（以下简称“我们”或“湖北 CA”）的产品/服务！我们非常重视您的个人信息保护。如我们提供的某款产品/服务有单独的隐私政策或当中存在特殊约定，则该产品/服务的隐私政策将优先适用，该款产品/服务中未涵盖的内容，以本政策内容为准。我们将通过本政策向您清晰地说明在使用我们的产品/服务时，我们如何收集、存储、保护、使用及对外提供您的个人信息，并说明您享有的权利，尽力保护您的个人信息安全可控。

本政策与您使用我们的产品/服务关系紧密，建议您在使用我们的产品/服务前，仔细阅读并了解本政策全部内容，做出您认为适当的选择，一旦您开始使用湖北 CA 产品/服务，即表示您已充分理解并同意本政策。我们对本政策中与您的权益存在重大关系的条款和敏感个人信息，采用突出显示（如加粗等）以提示您注意。

- 一、我们如何收集和使用您的个人信息
- 二、我们如何使用 Cookie 和同类技术
- 三、我们如何共享、转让、公开披露您的个人信息
- 四、我们如何保护和保存您的个人信息
- 五、您的权利
- 六、对第三方责任的声明
- 七、我们如何处理儿童的个人信息
- 八、本政策如何更新
- 九、如何联系我们

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。

敏感个人信息，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。

## 一、我们如何收集和使用您的个人信息

为了向您提供服务、保障服务的正常运行、改进和优化我们的服务以及保障帐号安全，我们会遵循“合法、正当、必要”原则，通过如下方式收集您的个人信息：

### 1. 注册用户收集的信息及使用

当您首次注册成为我们的用户时，您可能至少需要提供【手机号或邮箱等基本信息】，上述信息是为了帮助您完成用户注册。但如您有进一步服务需求，可能要补充提供【姓名、证件类型、证件号码、单位名称、统一社会信用代码等】。若您不提供这类信息，您将无法使用我们的服务。

### 2. 您在申请使用我们的服务时收集的信息及使用

在您使用我们以下各项业务功能（以下统称“服务”）的过程中，我们需要收集您的一些信息，用以向您提供服务、提升我们的服务质量、保障您的账户和资金安全以及符合国家法律法规及监管规定：

## 2.1 数字证书服务

在您申请我们为您签发、更新、吊销等数字证书服务时，如您是个人用户，您需向我们提供您的【姓名、身份证号码、实名手机号码、单位名称、通讯地址、银行账户信息、身份证件的影像、电子签名或印章的图样等信息】，如您是企业用户，您需向我们提供您的【企业名称、组织机构代码/统一社会信用代码、企业通讯地址、法定代表人及经办人的姓名、身份证号、手机号码、身份证件的影像、电子邮箱、单位银行对公账户信息等信息】。如您是事件型数字证书用户，除上述个人用户和/或企业用户需提供的信息外，您还需要向我们提供事件特征的数字摘要信息。

根据《电子认证服务管理办法》，我们需要向您核验身份时，您需向我们提供 2.2 中所列信息。这类信息用于核验您的身份，若您不提供这类信息，您将无法使用我们的数字证书服务。

## 2.2 身份核验服务

2.2.1 在您使用我们提供的身份核验服务前，我们将根据您所使用的不同身份核验方式收集您的相应信息。

如您是个人用户：

1) 当您使用运营商实名信息核验的身份核验方式时，我们会收集您的【姓名、实名手机号码、身份证号码】。

2) 当您使用银行卡鉴权的身份核验方式时，我们会收集您的【姓名、身份证号码、银行卡账号、银行预留手机号码】。

3) 当您使用生物识别特征比对的身份核验方式时，我们会收集您的【姓名、身份证号码、身份证照片/护照等证件照片、人脸面部影像信息或指纹信息或虹膜/巩膜信息】。

如您是企业用户，您还需要提供您的【营业执照/组织机构代码证等证照照片、对公银行账号，法定代表人及经办人的身份证/护照等证件照片等信息】，其中法定代表人及经办人需提供的信息种类参考上述不同身份核验方式。

若您不提供这类信息，您将无法使用我们的身份核验服务。

2.2.2 若您使用生物识别方式核验时，您需向我们提供您的生物识别信息，以核验您的身份：

a. 当您使用人脸登录方式时，我们会收集您的人脸面部影像信息。

b. 当您使用指纹登录方式时，我们会收集您的指纹信息。

c. 当您使用虹膜/巩膜登录方式时，我们会收集您的虹膜/巩膜信息。

如您不同意提供前述信息，您也可以选择其他核验方式。

您提供的上述信息，将在您使用我们服务期间持续授权我们使用。

## 2.3 电子签名或签章服务

在您使用我们提供的电子签名或签章服务前，您需向我们提供您的【数字证书信息、印章信息、印章图样或手写签名笔迹信息、待签署内容的原文或数字摘要信息、数字签名运算结果】，若您不提供这类信息，您将无法使用我们的电子签名或签章服务。

在您提供他人的信息时，您需确保已获得对方合法有效的授权且对方单独同意接受本政策之约束，因为您提供的信息造成他人损害的将由您承担全部责任。如果对方提出相反意见或者我们了解到信息主体不愿受本保护政策约束的，我们将删除相关信息。

您提供的上述信息，将在您使用我们服务期间持续授权我们使用。

## 3. 使用服务过程中收集的信息及使用

3.1 为了解产品适配性、识别账号异常状态，我们会收集关于您使用的服务以及使用方式的信息并将这些信息进行关联，这些信息包括：

1) **设备信息：**我们会根据您在软件安装及使用中授予的具体权限，接收并记录您

所使用的设备相关信息，例如设备型号、操作系统版本、设备设置、唯一设备标识符、Android ID 的特征信息等。

**2) 日志信息：**当您使用我们的服务时，我们会在后台运行状态下自动收集您对我们服务的详细使用情况，作为有关网络日志保存。例如您的搜索查询内容、IP 地址、浏览器的类型、网络运营服务商、使用的语言、访问日期和时间及您访问的网页记录等。

**3) 位置信息：**如您使用我们的电子签名或签章服务需要标记当前签名位置时，我们会收集您的位置信息，请开启位置使用权限。

**4) 使用相机：**如您需要使用相机拍摄时，您需开启相机使用权限。

**5) 相册：**如您需要从相册中选取证件或人像照片时，您需开启相册权限。

**6) 推送权限：**如您需要接收我们发送给您通知消息时，请开启推送权限。

**请您注意，您开启任一权限即代表您授权我们收集和使用与此相关的个人信息来为您提供对应服务，您一旦关闭任一权限即代表您取消了授权，我们将不再基于对应权限继续收集和使用相关个人信息，也无法为您提供该权限所对应的服务。但是，您关闭权限的决定不会影响此前基于您的授权所进行的信息收集及使用。**

3.2 当您与我们联系时，我们会保存您的通信/通话记录和-content或您留下的联系方式等信息，以便与您联系或帮助您解决问题，或记录相关问题的处理方案及结果。

如您已将个人信息提供给第三方业务机构，在获得您明确同意或授权情况下，该业务机构有权将上述信息提供给我们用于实现我们的服务。

#### **4. 为您提供安全保障或服务优化收集的信息及使用**

为提高您使用我们及我们合作伙伴提供服务的安全性，确保操作环境安全与识别注册账号异常状态，更好地保护您或其他用户或公众的人身财产安全免遭侵害，更好地预防钓鱼网站、欺诈、网络漏洞、计算机病毒、网络攻击、网络侵入等安全风险，更准确地识别违反法律法规或相关协议规则的情况，我们使用或整合您的用户信息、设备型号、IP 地址、设备软件版本信息、设备识别码、设备标识符、所在地区、网络使用习惯、第三方平台获取的必要身份标识以及其他与我们服务相关的日志信息以及我们合作伙伴取得您授权或依据法律共享的信息，来综合判断您账户及交易风险、进行身份验证、检测及防范安全事件，并依法采取必要的记录、审计、分析、处置措施。如您不同意我们记录前述信息，无法完成风控验证。

为了为您提供更优质的服务，我们会对收集的信息进行去标识化地研究、统计分析和预测，以用于改善我们的内容和布局，为商业决策提供产品或服务支撑，以及改进我们的产品和服务。

#### **5. 其他用途**

我们将基于本政策未载明的其他特定目的收集您的信息时，会事先告知并征求您的同意。我们收集及使用上述信息的目的是为了地更好地提供服务，您理解并同意，我们向您提供的功能不断优化升级的，如我们未在上述场景中明示您需要收集的个人信息，我们将会通过推送通知、弹窗、网站公告或者其他适当方式等方式另行向您告知并征得您同意。

#### **6. 收集、使用征得授权同意的例外**

根据相关法律法规规定，以下情形中收集、使用您的个人信息无需征得您的授权同意：

- 1) 与国家安全、国防安全等国家利益直接相关的；
- 2) 与公共安全、公共卫生、公众知情等重大公共利益直接相关的；
- 3) 与犯罪侦查、起诉、审判和判决执行等直接相关的；
- 4) 出于维护您或其他个人的生命、财产、声誉等重大合法权益但又很难得到本人

同意的；

5) 所收集的个人信息是您自行向社会公众公开的；

6) 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；

7) 用于维护所提供产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障；

8) 出于公共利益开展统计或学术研究所必要且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的；

9) 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；

10) 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；

11) 法律、行政法规规定的其他情形。

## 二、我们如何使用 Cookie 和同类技术

为使您获得更轻松、更快捷的访问体验，您使用我们产品/服务时，我们可能会通过采用各种技术收集和存储您访问我们产品/服务的相关数据，在您访问或再次访问我们产品/服务时，我们能识别您的身份，并通过分析数据为您提供更好更多的服务，包括使用小型数据文件识别您的身份，这么做是为了解您的使用习惯，帮您省去重复输入账户信息的步骤，或者帮助判断您的账户安全等。这些数据文件可能是 Cookie、FlashCookie 等，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”)。

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我们的 Cookie，但拒绝我们的 Cookie 在某些情况下您可能无法使用依赖于 cookies 的我们产品/服务的部分功能。

网页上常会包含一些电子图像，称为“单像素 GIF 文件”或“网络 beacon”，它可以帮助网站计算浏览网页的用户或访问某些 cookie。我们会通过网络 beacon 收集您浏览网页活动信息，例如您访问的页面地址、您先前访问的援引页面的地址、您停留在页面的时间、您的浏览环境以及显示设定等。

## 三、我们如何共享、转让、公开披露您的个人信息

### 1. 共享

我们不会与任何公司、组织和个人共享您的个人信息，但以下情况除外：

#### 1.1 事先获得您明确的同意或授权；

**1.2 与我们的关联公司共享：**您的个人信息可能会与我们的关联公司共享。我们只会共享必要的个人信息，且受本政策中所声明目的的约束。关联公司如要改变个人信息的处理目的，将再次征求您的授权同意。

我们的关联公司包括我们现在或将来控制、受控制或与其处于共同控制下的任何公司、机构以及上述公司或机构的合法继承人。其中“控制”是指直接或间接地拥有影响所提及公司管理的能力，无论是通过所有权、有投票权的股份、合同或其他被人民法院认定的方式。

**1.3 与授权的供应商和服务提供方（以下统称“第三方合作机构”）共享：**以下情形时我们在您使用服务时会将相关信息共享给第三方合作机构，以便完成对您提供服务。

1) 如您在其他业务机构的产品或服务中使用我们的数字证书，我们会向前述具体应用机构，提供您的数字证书中的信息（**作为个人用户：姓名、身份证号码、工作单位名称、证书序列号等；作为企业用户：企业名称、组织机构代码、法定代表人姓名、证书序列号等**），以便您的数字证书能够在具体应用中有效使用。

2) 如您在其他业务机构的产品或服务中使用我们的数字证书且数字证书有效期即将届满，我们可能会向前述具体应用机构，提供您的数字证书中的信息（**作为个人用户：姓名、身份证号码、工作单位名称、证书序列号等；作为企业用户：企业名称、组织机构代码、法定代表人姓名、证书序列号等**）及手机号码，用于证书更新服务提醒。事件型证书不涉及本项服务。

3) 如您通过其他业务机构申请开具办理证书的发票时，我们会向前述具体应用机构提供您的【姓名/名称、纳税人识别号、电子邮箱等基本信息】。

我们可能会根据法律法规规定、诉讼争议解决需要，或按政府主管部门、监管机构、司法机关、证券交易所的依法提出的要求，提供您的个人信息。

请您知悉，即使已经取得您的授权同意，我们也仅会出于合法、正当、必要、明确的目的共享您的个人信息。

## 2. 委托处理

以下情形，我们将委托第三方合作机构处理您的信息：

**2.1 当您通过运营商实名信息核验进行身份核验时，我们委托第三方合作机构验证您的【姓名、实名手机号码、身份证号码】。**

**2.2 当您通过银行卡鉴权的身份核验方式进行核验时，我们委托第三方合作机构验证您的【姓名、身份证号码、银行卡账号、银行预留手机号码】。**

**2.3 当您通过生物识别特征比对的身份核验方式进行核验时，我们委托第三方合作机构验证您的【姓名、身份证号码、身份证照片/护照等证件照片、人脸面部影像信息、指纹信息、虹膜/巩膜信息】。**

**2.4 当您通过企业信息核验方式进行核验时，我们委托第三方合作机构验证企业信息，包括【企业名称、统一社会信用代码、法定代表人姓名及身份证号等信息】。**

委托处理过程中，我们将评估该第三方合作机构收集信息的合法性、正当性、必要性。我们将要求第三方合作机构对您的信息采取保护措施，并且严格遵守相关法律法规与监管要求。

对受我们委托处理您的个人信息的第三方合作机构，我们会与其签署严格的保密条款要求他们按照我们的要求、本政策以及其他任何相关的保密和安全措施来保护您的个人信息。

## 3. 转让

我们不会将您的个人信息转让给任何公司、组织和个人，但以下情况除外：

3.1 事先获得您的明确同意或授权；

3.2 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。

## 4. 公开披露

我们仅会在以下情形，公开披露您的个人信息：

4.1 在您明确同意或主动选择情况下，我们根据您授权情况公开披露您所指定的个人信息；

4.2 为了标识您的网络身份，我们会在数字证书中记载您的姓名、工作单位名称、手机号码、身份证件号码等身份信息；

4.3 根据《电子认证服务管理办法》规定，我们通过证书信息查询服务提供证书信息的在线查询，您本人和其他依赖方可通过我们的证书信息查询平台查看您数字证书中

的信息；

4.4 根据法律、法规的要求、强制性的行政执法或司法要求所必须提供您个人信息的情况下，我们依据要求公开披露您的个人信息。在符合法律法规的前提下，当我们收到上述披露信息的请求时，我们会要求必须出具与之相应的法律文件或依据，如传票或调查函。

#### **5.共享、转让、公开披露个人信息时事先征得授权同意的例外**

以下情形中，共享、转让、公开披露您的个人信息无需事先征得您的授权同意：

5.1 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；

5.2 为履行法定职责或者法定义务所必需；

5.3 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；

5.4 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；

5.5 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；

5.6 法律、行政法规规定的其他情形。

根据法律规定，经匿名化处理的个人信息，且确保数据接收方无法复原并重新识别个人信息主体的，不属于个人信息，对此类数据的处理将无需另行向您通知并征得您的同意。

## **四、我们如何保护和保存您的个人信息**

4.1 我们在中华人民共和国境内收集和产生的个人信息将存储在中华人民共和国境内。如部分服务涉及跨境业务，我们需要向境外机构传输境内收集的相关个人信息的，我们会按照法律法规和相关监管部门的规定执行，向您说明个人信息出境的目的以及涉及的个人信息类型，单独征得您的授权同意，并通过签订协议、核查等有效措施，要求数据接收方/境外机构采取安全保密措施处理个人信息。除非获得您的同意，并满足法律规定的评估及许可等法定程序，我们不会跨境传输您的个人信息。

**4.2 我们会采取一切合理可行的措施，确保未收集无关的个人信息。我们只会在达成本政策所述目的所需的期限内保留您的个人信息。**

但在下列情况下，我们有可能因需符合法律要求，更改个人信息的存储时间：

- 1) 为遵守适用的法律法规等有关规定；
- 2) 为遵守法院判决、裁定或其他法律程序的规定；
- 3) 为遵守相关政府机关或法定授权组织的要求；

对于您使用数字证书服务中提供的个人信息，我们会按照《电子签名法》的规定妥善保管。为了便于数字证书服务的事后证明，我们可能会延长保管期限。

4.3 如我们停止运营我们的服务，我们将及时停止继续收集和使用您的个人信息的活动，将停止运营的通知以公告的形式通知您，并在合理期限内对我们所持有的您的个人信息进行删除或匿名化处理。

法律法规有规定不能删除时或不能匿名化处理的情况除外，包括我们拟暂停或者终止电子认证服务时，我们需按照监管部门的要求对您在使用我们的电子认证服务期间提供或产生的信息移交至承接我们业务的其他电子认证服务机构。

4.4 我们已使用符合业界标准的安全防护措施保护您提供的个人信息，防止数据遭到未经授权的访问、公开披露、使用、修改、损坏或丢失。我们会采取一切可行的措施，保护您的个人信息。例如：我们采取了合适的管理、技术以及物理安全措施，在数据收

集、存储、显示、处理、使用、销毁等各个环节建立了安全防护措施，根据信息敏感程度的级别采取不同的控制措施，包括但不限于通过网络安全层软件（SSL）进行加密传输、信息加密存储、严格限制数据中心的访问等，建立了与业务发展相适应的信息安全保障体系。

**4.5** 我们建立了相关内控制度，对可能接触到您的信息的工作人员采取最小够用授权原则；对工作人员处理您的信息的行为进行系统监控，不断对工作人员培训相关法律法规及隐私安全准则和安全意识强化宣导。

**4.6 请您务必妥善保管好您的个人信息，尤其是用于身份核验的信息（如生物识别信息、短信验证码等）。一旦您泄漏了前述信息，您可能会蒙受损失，并可能对您产生不利。如您发现个人信息要素可能或已经泄露时，请您立即和我们取得联系，以便我们及时采取相应措施以避免或降低相关损失。**

**4.7 请您理解：**互联网环境并非百分之百安全，我们将尽力确保或担保您发送给我们的任何信息的安全性，但由于技术的限制及可能存在的各种恶意手段，即便竭尽所能加强安全措施，也不可能始终保证信息百分之百安全。如果不幸发生我们的物理、技术或管理防护措施遭到破坏的事件，我们会及时启动应急预案，防止安全事件扩大，按照法律法规的要求上报国家主管机关，并及时采取推送、公告等合理、有效的方式向您告知安全事件的基本情况、可能的影响、已经采取的措施或将要采取的措施等。

## 五、您的权利

### 5.1 查阅、更正您的个人信息

我们鼓励您更新和补充您的信息以使其更准确有效。您有权查阅、复制您的信息，并根据对应信息的管理方式自行完成或要求我们在符合法律规定和监管规定的前提下进行修改和补充。您可以发送电子邮件至 [hbca@hbca.org.cn](mailto:hbca@hbca.org.cn)，我们将在 15 天内回复您的请求。我们将采取适当的技术手段，尽可能保证您可以访问、更正自己的信息。

### 5.2 删除您的个人信息

在以下情形中，您可以向我们提出删除个人信息的请求：

- 1) 处理目的已实现、无法实现或者为实现处理目的不再必要；
- 2) 个人信息处理者停止提供产品或者服务，或者保存期限已届满；
- 3) 个人撤回同意；
- 4) 个人信息处理者违反法律、行政法规或者违反约定处理个人信息；
- 5) 法律、行政法规规定的其他情形。

若我们决定响应您的删除请求，我们还将同时通知从我们获得您的个人信息的实体，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信息后，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。

### 5.3 改变您授权同意的范围

您可以通过关闭设备功能来撤回您的授权。您也可以通过注销账户的方式，撤回我们继续收集和使用您个人信息的全部授权。

当您收回同意后，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已进行的个人信息处理。

### 5.4 个人信息主体注销账户

在您需要终止使用我们的服务时，您可以发送电子邮件至 [hbca@hbca.org.cn](mailto:hbca@hbca.org.cn)，经验证您的真实身份后再决定注销您的账户。我们在此善意地提醒您，您注销账户的行为会使您无法继续使用我们的服务。注销账户后您的个人信息会保持不可被检索、访问

的状态，我们将不会再收集、使用或共享与该账户相关的个人信息。但已采集的信息如法律法规有规定的我们仍需按照规定时限和方法进行保存，且在保存的时间内依法配合有权机关的查询。

#### 5.5 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：本人携带身份证至湖北 CA 现场，或通过邮寄本人申请文件，湖北 CA 将以邮寄、电子邮件、现场复印等方式提供副本。

#### 5.6 响应您的上述请求

为保障安全，您需要提供书面请求，或以其他方式证明您的身份。我们会先验证自己的身份，然后再处理您的请求。我们将在验证您的身份后十五天内作出答复。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，我们将视情况收取一定成本费用。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。

在以下情形中，我们将无法响应您的请求：

- （1）与个人信息控制者履行法律法规规定的义务相关的；
- （2）与国家安全、国防安全直接有关的；
- （3）与公共安全、公共卫生、重大公共利益直接有关的；与刑事侦查、起诉、审判和判决执行等直接有关的；
- （4）有充分证据表明您存在主观恶意或滥用权利的；
- （5）出于维护您或其他个人的生命、财产等重大合法权益又很难得到本人授权同意的；
- （6）响应您的请求将导致您或其他个人、组织的合法权益受到严重损害的；
- （7）涉及商业秘密的。

### 六、对第三方责任的声明

请您注意，您的交易相对方、您访问的第三方网站经营者、通过我们接入的第三方服务可能有自己的信息保护政策；当您查看第三方创建的网页或使用第三方开发的应用程序时，这些第三方可能会放置他们自己的 Cookie 或网络 Beacon，这些 Cookie 或网络 Beacon 不受我们的控制，且它们的使用不受本政策的约束。我们会努力去要求这些主体对您的个人信息采取保护措施，建议您与他们联系以获得关于他们的信息保护政策的详细情况。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我们的要求采取措施，您应当仔细阅读他们的服务协议及个人信息保护政策。如您发现这些第三方创建的网页或第三方开发的应用程序存在风险时，建议您终止相关操作以保护您的合法权益。

### 七、我们如何处理儿童的个人信息

我们的产品、网站和服务主要面向成人。如果没有父母或监护人的书面同意，儿童不应使用我们的服务。

对于经父母或其他监护人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、父母或其他监护人明确同意或者保护儿童所必要的情况下使用或公开披露此信息。

尽管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或其他监护人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。如您认为我们可能在未经您同意的情况下收



集了您监护的未成年被监护人的信息或若您和您的监护人对此有相关疑问, 请通过本政策公布的联系方式与我们联系。我们核实后会对收集的未成年人的个人信息予以删除。

## 八、本政策如何更新

**8.1 我们所有的服务/产品均适用本政策, 除非相关服务/产品已有独立的信息保护政策或相应的用户服务协议当中存在特殊约定。**

**8.2 我们的个人信息保护政策可能变更。当本政策的条款发生变更时, 我们将以公告的形式或以其他适当方式来通知您, 新政策公布之日即为生效日期。如您在本政策更新生效后继续使用我们的服务, 即表示您已充分阅读、理解并接受更新后的政策并愿意受更新后的政策约束。**

本政策所指的重大变更包括但不限于:

- 1) 我们的服务模式发生重大变化, 如处理用户信息的目的、用户信息的使用方式等;
- 2) 我们在控制权、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;
- 3) 用户信息共享、转让或公开披露的主要对象发生变化;
- 4) 我们负责处理用户信息安全的责任部门、联络方式及投诉渠道发生变化时;
- 5) 用户信息安全影响评估报告表明存在高风险时;
- 6) 其他可能对您的个人信息权益产生重大影响的变化。

## 九、如何联系我们

如果您对我们的个人信息政策或数据处理有任何疑问、意见或建议, 可以通过以下方式与我们联系, 我们联系方式:

湖北省数字证书认证管理中心有限公司

公司地址:武汉市武昌区华中小龟山金融文化公园 9 栋

E-mail: hbca@hbca.org.cn

服务热线:400-870-8080

受理时间: 工作日 上午 8:30-12:00 下午 13:30-17:30

我们将尽快审核所涉问题, 并在验证您的用户身份后 30 天内予以回复。如果您对我们的回复不满意, 特别是我们的个人信息处理行为损害了您的合法权益, 首先应友好协商解决, 协商不成的, 双方同意纠纷或争议受我们工商注册所在地的人民法院管辖。