

# 隐私政策

最后更新日期：2024 年 11 月 11 日

欢迎您使用亚数信息科技（上海）有限公司（以下称“亚数信息” “亚洲诚信” “TrustAsia” 或 “我们”）的产品和服务！我们深知个人信息对您的重要性，并会尽全力保护您的个人信息安全可靠。我们致力于维持您对我们的信任，恪守以下原则，保护您的个人信息：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、公开透明原则等。同时，

亚数信息承诺，我们将按业界成熟的安全标准，采取相应的安全保护措施来保护您的个人信息。请在使用我们的产品或服务前，仔细阅读并了解本《隐私政策》（以下称“本政策”）。

本政策将向您说明我们如何收集、使用、共享、披露您的个人信息，我们如何存储及采取安全措施保护您的个人信息，以及您对您的个人信息所拥有的管理权利及实现方式。除本政策外，**在特定场景下，我们还会通过即时告知（含弹窗、页面提示等）、功能更新说明等方式，向您说明对应的信息收集目的、范围及使用方式，这些即时告知及功能更新说明等构成本政策的一部分，并与本政策具有同等效力。**

在您开始使用我们的产品和服务前，请您务必先仔细阅读（未成年人请在监护人陪同下阅读）和理解本政策，特别应重点阅读我们以粗体/粗体下划线标识的条款，确保您充分理解和同意之后再开始使用。**尤其是当您通过本政策适用的相关页面主动向我们提供您的个人信息或通过相关操作行为表示同意我们收集您的个人信息时，我们有充分、合理的理由认为您已充分阅读、理解并同意接受本政策的约束。在您自主使用本网站及相关服务时，本政策即在您与我们之间产生法律效力。**

本政策将帮助您了解以下内容：

- 一、本政策的适用范围
- 二、我们如何收集和使用您的个人信息
- 三、我们如何使用 COOKIES 或同类技术
- 四、我们如何共享、转让和披露您的个人信息

- 五、我们如何保护和保存您的个人信息
- 六、您的权利
- 七、第三方服务
- 八、未成年人保护
- 九、我们对去世用户的个人信息保护
- 十、您的个人信息如何在全球范围内转移
- 十一、通知和修订
- 十二、如何联系我们

## **一、本政策的适用范围**

本政策适用于亚数信息及其关联方旗下各类网站、APP、小程序以及随技术发展出现的新形态（以下统称为“TrustAsia 应用”）向您提供的各类产品、服务和应用。若我们向您提供的产品、服务或应用内设有单独隐私政策或类似法律文件，该等政策/文件与本文件共同构成亚数信息隐私政策，如条款之间存在冲突的，以单独隐私政策或类似法律文件为准。

本协议仅适用于您在使用 TrustAsia 应用及相关服务的过程中所涉及的**个人信息**，包括归属于您本人的个人信息以及归属于其他个人、但经由您获得**个人主体的授权后提交的个人信息**，针对其他归属于实体单位的信息，我们将按照与对应实体单位签署的合同或协议或通过其他方式达成一致的约定进行处理。

本政策不适用于其他第三方通过 TrustAsia 应用或其他方式向您提供的产品或服务（例如微信、支付宝、其他支付平台或任何第三方网站、通过 TrustAsia 应用提供广告服务的公司）。当您使用其他第三方向您提供的产品或服务时，您需与该第三方另行就产品或服务使用相关的权利义务协商达成一致。

**需特别说明的是，作为我们的用户，若您利用我们的产品、技术、服务，为您的用户再行提供产品、服务，您应当依照相关法律要求另行与您的用户约定隐私权政策或类似法律文件。**

我们收集实现产品功能所需要的信息，并将收集信息进行合理使用。

## **二、我们如何收集和使用您的个人信息**

## （一）我们如何收集您的个人信息

在您使用 TrustAsia 应用及相关服务的过程中，可能涉及您的个人信息的具体情况如下：

**1.您主动提供的信息：** 我们将收集并存储您在使用 TrustAsia 应用时向我们主动提供的信息，包括您主动填写的信息、购买产品/服务或与我们联系时产生的信息。

**2.我们主动收集的信息：** 在使用 TrustAsia 的产品、服务和应用的过程中，我们会根据相关法律法规和您的授权范围收集您的设备、位置等信息。

**3.我们通过第三方获取的信息：** 我们还可能从关联方、合作方、信用机构以及其他依法成立并合法留存您的相关信息的第三方机构获取您的相关信息。

## （二）我们如何使用您的个人信息

我们为您提供包括但不限于业务咨询、电子认证、数字证书、身份鉴别、电子签名、密码技术、区块链及其衍生产品和技术服务。在您使用前述各项服务时，我们需要根据服务内容的不同分别收集您的不同内容的信息，我们收集您信息的范围仅限于为您提供对应服务所必需的相关资料，以便给您提供各项服务，提升我们的服务质量以及符合国家法律法规及监管规定。

我们提供的具体服务类型及相应收集的信息内容如下：

个人信息	使用目的	处理的法律依据
姓名、国别、手机号码、电子邮箱、接受验证码、用户名、APPID	我们使用这些信息来： 根据您的请求为您创建一个账户，和/或验证您是否拥有一个账户； 允许密码重置； 向您提供用户支持； 记录交易或提供订单确认；以及 执行我们的条款、条件和政策。	我们会处理此类信息，因为这对于我们履行与您签订的合同以便提供服务而言是必要的。
姓名、职位、邮箱、电话、辅助证明个人身份的证明文件（必要时）、身份证/护照/驾照（外籍人士）、用户名、本人手持身份证/护照/驾照（外籍人士/持国外绿卡人士）持证件照片	我们使用这些信息来： 用于颁发证书时鉴别您/您所在企业的身份信息、CSA 会员信息、展示组织信息	我们会处理此类信息，因为这对于我们履行与您签订的合同以便提供服务而言是必要的。

手机号码、用户名	我们使用这些信息来： 验证您是否拥有一个账号。	我们会处理此类信息，因为这对于我们履行与您签订的合同以便提供服务而言是必要的。
交易记录（如支付服务费用的日期和时间）（必要信息）、银行卡信息、支付宝、微信支付第三方账号信息（敏感个人信息）	用于核对账单、订单支出等信息。我们为您提供访问您交易记录的权限，以便您查看您的交易历史记录。	我们会处理此类信息，因为这对于我们履行与您签订的合同以便提供服务而言是必要的。
日志信息、设备信息、OCSP 查询服务	我们使用此类信息来改善我们的服务和响应。	改进我们的战略和服务符合我们的合法权益。

## 1. 用户注册：

**1)成为 TrustAsia 应用的注册用户：**您可在 TrustAsia 应用的账号注册页面，通过提交您的姓名、国别、手机号码及电子邮箱、接受验证码等以创建账号，

成为 TrustAsia 应用的注册用户可以帮助我们为您提供所需的相关服务，如您未提供对应信息，您将无法使用我们对应的服务。

**2)实名认证：**如您进行实名认证，我们还会收集您的身份证/护照等证件照片、脸部图像、声音、视频及其他需要您提供的认证信息。如您是企业用户，您需要提供您的证照照片、对公银行账号、法定代表人/负责人及授权经办人的身份证/护照等证件照片。如您不提供此类信息，我们将无法为您提供电子认证、数字证书、身份鉴别、密码技术、区块链技术相关产品与/或服务。

**3)为您提供信息反馈渠道，具体包括：**如您希望向我们咨询证书申请、证书续费、售后服务、成为 TrustAsia 的合作伙伴、自动部署等相关问题，您可直接通过 TrustAisa 网站页面直接与我们的在线客服沟通或通过热线电话咨询产品/服务购买或使用相关问题，在线交谈过程中为便于我们与您进一步联系，我们可能需要您提供**联系方式**等相关个人信息，您可根据自身需求自行决定是否提供。

## 2. 产品、服务购买

**1)数字证书服务。**在您购买我们的数字证书产品和服务时，我们需要您提供您的部分个人信息（例如姓名、电话号码、身份证号码、手持身份证视频/

**照片、电子邮箱)** 以完成证书的申请及签发核验。

另外，为便于向您交付数字证书或服务，您至少需按照提示向我们提供**证书信息、服务期限信息、支付状态信息**。收集上述的信息是为了满足相关法律法规和证书签发的要求，若您不提供这类信息，仅会使您无法使用取得相关证书产品，但不影响您在对应网站浏览、查询或使用其他功能。

同时，为了验证您提供信息的准确性和完整性，我们会与合法留存您信息的国家机关、金融机构、企事业单位进行核对，如在验证核对过程中我们需要向前述验证机构收集您的信息，我们会依照法律法规或监管规定要求相关验证机构说明其个人信息来源，并对其个人信息来源的合法性进行确认。

**2)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。

**3)实名认证服务。** 在您使用我们提供的身份核验服务前，如您是个人用户，您需向我们提供您的姓名、银行账户信息、实名手机号、身份证正反面照片及身份证上所有信息(姓名、性别、民族、出生日期、住址、公民身份号码、本人照片、签发机关、证件的有效期限)，如您为外籍人士，您将需要提供您的护照相关页信息以供核验认证以及您的脸部图像、声音、视频等身份核验信息的一项或者多项，如您是企业用户，您需向我们提供企业法定代表人及经办人的姓名、身份证号、手机号中的一项或者多项。若您不提供这类信息，您将无法使用我们的身份核验服务。

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也同意接受本政策之约束，由您提供的信息造成他人损害的将由您承担全部责任。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。如果信息所有人提出相反意见或者我们了解到信息所有人不愿受本政策约束的，我们将删除相关信息。需要特别说明的是，如相关法律法规政策有特殊要求的，信息将根据政策要求保留对应年限。比如，针对数字证书产品，国内电子认证服务数据至少保留至证书过期后五年，国际电子认证服务数据至少保留至证书过期后二年（Matter 电子认证服务数据至少保留至证书过期后五年）。

### 3.关于您使用的服务以及使用方式的信息：

在您使用我们服务过程中，为识别账号异常状态、了解产品适配性，向您提供浏览、搜索等基本服务，保障服务正常运行，优化服务体验，我们可能会直接或间接地收集、存储关于您使用的服务以及使用方式的信息并将这些信息关联，这些信息包括：

**1)日志信息：**当您使用我们的各类服务时，我们会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。例如您的登录账号、搜索查询内容、IP 地址、浏览器的类型、网络环境、使用的语言、访问时间及您访问的网页浏览记录、停留时长、刷新纪录等。

**2)设备信息：**我们可能会在您使用我们服务时，接收并记录您所使用的设备相关信息，例如操作系统及版本、客户端版本、设备标识符（MAC 地址等信息）、所在位置相关信息（例如 IP 地址信息）。

**3)数字证书管理服务：**在您使用我们的相关产品或者服务进行数字证书操作和管理的过程中，我们需要收集您使用过程中产生的浏览和操作历史等数据。

**4)OCSP 查询服务：**当您使用的相关产品或者服务包含 OCSP 查询功能时，我们需获取您的部分网络信息，如设备标识、版本、IP 等信息。

**5)消息通知：**对于您在使用应用、服务的过程中提供的联系方式（例如：联系邮箱、电话），我们在运营中可能会向其中的一种或多种发送多类通知，用于用户消息告知、身份验证、安全验证、用户使用体验调研等用途；此外，我们也可能会以电子邮件、短信、电话的方式，向您发送您可能感兴趣的服务、功能或活动的商业性信息。如您不愿接受这些信息，您可以通过产品或者服务平台或者邮件中提供的退订方式进行退订。

**6)支付结算：**如您在我们的服务过程中产生支付结算，支付结算过程中，您可以选择我们的关联方或与我们合作的第三方支付机构（包括支付宝支付、微信支付、Apple Pay 及银联、网联等支付通道，以下称“支付机构”）所提供的支付服务。支付服务过程中我们可能需要将您在我们服务中的订单号与交易金额信息同这些支付机构共享以实现其确认您的支付指令并完成支付。

**7)订单信息管理：**为展示您账户的订单信息及保障您的售后权益，我们会收集您在使用我们服务过程中产生的**订单信息、交易和消费记录、虚拟财产信**

**息（敏感个人信息）** 用于向您展示及便于您对订单进行管理。如发生交易退费情形的，我们可能会要求您提供您的银行账号信息，包括**银行卡信息、支付宝、微信支付第三方账号信息（敏感个人信息）** 用于为您处理退费请求。

**8)交易状态确认及售后争议解决：** 为确认交易状态及为您提供售后与争议解决服务，我们会通过您基于交易所选择的交易对象、支付机构等收集与交易进度相关的**您的交易、支付信息**，并将您的上述交易、支付信息共享给相关的上述服务提供者。

**9)客户响应：** 当您联系我们的客服或使用其他用户响应功能时（例如提出售后申请、个人信息保护投诉或建议、其他客户投诉和需求），我们可能需要您提供必要的个人信息以匹配并核验您的用户身份，以便保障您的账号与系统安全。我们可能还会保存您的**联系方式（敏感个人信息）（您与我们联系时使用的或您向我们主动提供的其他联系方式）、您与我们的通信/通话记录内容以及您在平台响应功能中反馈的内容（包括文字/图片/音视频/通话记录等形式）、与您需求相关联的其他必要信息**，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。

**10)为您提供安全保障：** 为提高您使用我们及合作伙伴提供服务的安全性，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我们服务相关协议规则的情况，我们可能会收集、使用或整合您的**账户信息、交易信息、设备信息、日志信息以及我们关联公司、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。

**11)改进我们的服务：** 我们可能让您参与有关我们服务的调查，帮助我们改善现有服务或设计新服务；同时，我们可能将您的信息用于网站更新。

**12)出于其他合理且必要的目的：** 如果某一需要收集您的个人信息的产品/服务未能在本隐私政策中予以说明的，或者我们超出了与收集您的个人信息时所声称的目的及具有直接或合理关联范围的，我们将在收集和您的个人信息前，通过更新本隐私政策、页面提示、弹窗、站内信、网站公告或其他便于

您获知的方式另行向您说明，并为您提供自主选择同意的方式，且在征得您明示同意后收集和使用。

**您了解并同意，单独的设备信息、日志信息是无法识别特定自然人身份的信息。如果我们将前述信息与其他个人信息结合用于识别特定自然人身份，或者将其与能够识别自然人身份的信息结合使用，则在结合使用期间，除取得您授权或法律法规另有规定外，我们会将该类个人信息做匿名化、去标识化处理。这些信息在结合使用期间，我们将其按照本政策予以处理与保护。**

#### **4. 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) 履行法律法规规定的义务相关的；
- 2) 与国家安全、国防安全直接相关的；
- 3) 与公共安全、公共卫生、重大公共利益直接相关的；
- 4) 与刑事侦查、起诉、审判和判决执行等直接相关的；
- 5) 为订立、履行您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的；
- 6) 出于维护您或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；
- 7) 所收集的个人信息是您自行公开或其他已经合法公开的；
- 8) 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；
- 9) 根据您的要求签订和履行合同所必需的；
- 10) 开展合法的新闻报道所必需的；
- 11) 法律法规规定的其他情形。

### **三、我们如何使用 COOKIES 或同类技术**

为确保服务正常运转、为您获得更轻松 的访问体验，我们可能通过 COOKIES 或同类技术获取和使用您的信息，并将该等信息存储为日志信息。COOKIES 是少量的数据，它们从一个网络服务器送至您的浏览器并存在计算机



硬盘上。我们使用自己的COOKIES 或同类技术，可能用于以下用途：

1.记住您的身份。例如：COOKIES 或同类技术有助于我们辨认您作为我们的注册用户的身份，或保存您向我们提供有关您的喜好或其他信息；

2.分析您使用我们服务的情况。我们可利用 COOKIES 或同类技术来了解您使用服务进行什么活动、或哪些服务。

您应该能够控制 COOKIES 是否以及怎样被您的浏览器接受。请查阅您的浏览器附带的文件以获得更多这方面的信息。如果您拒绝我们使用 COOKIES 及同类技术收集和使用您的相关信息，您可通过浏览器设置管理或拒绝 COOKIES 与/或同类技术；或删除已经储存在您的计算机、移动设备或其他装置内的 COOKIES 与/或同类技术。

**您理解并知悉：我们的某些产品/服务只能通过使用 COOKIES 或同类技术才可得到实现，如您拒绝使用或删除的，您可能将无法正常使用我们的相关产品/服务或无法通过我们的产品/服务获得最佳的服务体验，同时也可能会对您的信息保护和账号安全性造成一定的影响。**

#### **四、我们可能共享、 转让和披露的个人信息**

##### **(一) 共享**

我们非常重视保护您的个人信息。我们不会与我们之外的任何第三方共享您的信息，但以下情形除外：

1.事先获得您明确的同意、授权或应您合法需求及同意；

2.为实现我们的合同目的/服务/功能所必须。在某些情况下，我们需向第三方共享您的信息，以实现我们产品与/或服务的功能，让您正常使用您需要的服务，包括：

1)向提供支付服务的第三方支付机构共享对应的交易订单信息和支付金额信息；

2)为向您提供特定产品和服务以满足合同目的所必须，向对应供应商、服务提供商、合作伙伴和节点运营商共享，以处理您提供的个人信息，获得比对结果，并最终向您提供特定产品和服务。在您知悉并明示同意的情况下，我们将向您收集并共享部分个人信息，具体包括：**经办人姓名、手机号码、邮箱、**

**职位、身份证件号码以及本人手持身份证照片或录像；如您是代表某家或多家企业购买特定产品及服务，您还需提供对应企业法定代表人姓名及身份证号、经办人身份核验信息、辅助证明个人身份的证明文件（必要时），您需告知并取得个人信息主体明确同意，即为实现合同目的/服务/功能所必须，我们需要向对应供应商、服务提供商、合作伙伴和节点运营商共享，以处理您提供的个人信息，获得比对结果，并最终向您提供特定产品和服务。**

3.关联方共享：为便于您进行统一管理、保障系统和帐号安全等，您的个人信息可能会在我们的关联方之间进行必要共享，包括：

1)您的帐号信息会在我们和我们的关联方的产品内部进行必要共享以帮助您节省时间、简化操作流程；

2)您的帐号信息、设备信息、相关浏览数据等反映您使用习惯和爱好的信息可能会与我们的关联方共享以使您在我们及关联方产品、服务、应用中有一致性和个性化的浏览、广告等服务体验。

4.实现本政策第一条“我们如何收集和使用您的个人信息”部分所述的其 他目的。

5.履行双方在本政策/其他协议（包括在线签署的电子协议以及相应的平台规则）中的约定。

6.为遵守法律法规的相关规定或为维护国家利益、社会公众利益、在遵守相关法律法规的前提下为我们及关联方或合作伙伴的商业秘密、您或其他服务用户的财产或安全免遭损害等（比如为防止欺诈等违法活动和减少信用风险），我们可能与第三方交换信息。前述信息不包括为获利目的出售、出租、共享或以其它方式而披露的信息。

7.应您的监护人合法要求。

**我们仅出于合法、正当、必要、特定、明确的目的共享您的个人信息。我们会与共享个人信息的第三方签署严格的保密协议，要求其按照以同等水平或更高的保密措施来处理您提供的个人信息。**

## **（二）转让**

如果我们出售或购买任何企业或发生合并，我们将向第三方披露信息，在这种情况下，我们将向此类企业的潜在买家披露您的数据。如果我们与其他公

司或企业进行买卖、合并或合作，或出售部分或全部资产，我们也会向第三方披露信息。在此类交易中，用户信息可能包含在转让资产中。如发生前述情形，我们将通过网站公告等形式向您提前告知。

### **(三) 披露**

在采取符合业界标准的安全防护措施并发生以下情况时，我们才会披露您的信息：

- 1.根据您的需求，在您明确同意的披露方式下披露您所指定的信息；
- 2.根据法律法规和相关行政、执法部门的要求，必须提供您个人信息的，我们可能会根据要求的信息类型和披露方式披露您的信息。当我们收到上述披露您提供的个人信息的请求时，我们会在符合法律法规的前提下，要求接收方必须出具相应的法律文件，如传票或调查函等。我们对所有的请求都进行慎重的审查，在确保相关请求具备合法依据且对应机构因特定调查目的有权合法获取该等个人信息的情况下，向其提供您对应的个人信息。

### **(四) 事先征得授权同意的例外**

以下情形中，共享、转让、披露您的信息无需事先征得您的授权同意：

- 1.与国家安全、国防安全、公共安全、公共卫生、重大公共利益直接相关的；
- 2.与刑事侦查、起诉、审判和判决执行等直接相关的；
- 3.为订立、履行您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的；
- 4.为履行法定职责或者法定义务所必需的；
- 5.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的；
- 6.在合理范围内处理您自行公开或者其他已经合法公开的个人信息，对您的权益有重大影响或您明确拒绝的除外；
- 7.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您的个人信息的；
- 8.法律法规规定的其他情形。

根据法律规定，共享、转让、披露经去标识化处理的个人信息，且确保数

据接收方无法复原并重新识别个人信息主体的，不属于个人信息的对外共享、转让及公开披露行为，对此类数据的保存及处理将无需另行向您通知并征得您的同意。

## **五、我们如何存储和保护个人信息**

### **(一) 个人信息的存储**

#### **1.信息存储的地点**

我们在中华人民共和国境内运营中收集和产生的信息，存储在中华人民共和国境内，以下情形除外：

1)法律法规有明确规定；

2)获得您的授权同意；

3)为实现合同目的所必须，您购买/使用的产品、服务确需向境外机构传输境内收集的相关个人信息的。针对个人信息出境的情形，我们与我们的合作方、供应商遵守在不同国家/地区之间传输个人信息的适用法律，确保您的个人信息得到足够的保护，例如匿名化、安全存储等。

#### **2.信息存储的期限**

在您使用我们的产品与/或服务期间，您的个人信息将在收集或使用个人信息的目的已经实现期限内保存，同时将结合法律有强制的留存要求期限的规定确定，如按照《中华人民共和国电子签名法》的相关要求信息保存期限至少为电子签名认证证书失效后 5 年。在超出保存期间后，我们会根据适用法律的要求删除您的个人信息，或进行匿名化处理。

#### **3.信息存储的方式**

以纸质、电子、光学、磁或者类似手段储存。

### **(二) 个人信息的保护**

我们非常重视个人信息安全，我们使用各种安全技术和程序，并采取一切合理可行的措施，保护您的信息，以防信息的丢失、不正当使用、未经授权阅览或披露。

#### **1.数据安全保护措施**

我们采用符合业界标准的安全防护措施，包括建立合理的制度规范、安全技术来防止您的信息遭到未经授权的访问使用、修改，避免数据的损坏或丢失。

网络服务采取了多种加密技术，例如在某些服务中，我们将利用加密技术（例如 TLS）来保护您的信息，采取加密技术对您的信息进行加密保存，并通过隔离技术进行隔离。在信息使用时，例如信息展示、信息关联计算，我们会采用多种数据脱敏技术增强信息在使用中安全性。采用严格的数据访问权限控制和多重身份认证技术保护信息，避免数据被违规使用。

## **2.其他安全措施**

我们通过建立数据分类分级制度、数据安全管理制度、数据安全开发规范来管理规范信息的存储和使用。

我们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。

加强安全意识。我们定期举办安全和隐私保护培训课程，加强员工对于个人信息保护政策和相关规程的认识。

我们仅允许有必要知晓这些信息的员工、合作伙伴访问您的信息，并为此设置严格的访问权限控制和监控机制。我们同时要求可能接触到您的信息的所有人员履行相应的保密义务。如果未能履行这些义务，可能会被追究法律责任或被中止与我们的合作关系。

## **3.安全事件处置**

为应对个人信息泄露、损毁和丢失等可能出现的风险，我们制定了多项制度，明确安全事件、安全漏洞的分类分级标准及相应的处理流程。我们也为安全事件建立了专门的应急响应团队，按照安全事件处置规范要求，针对不同安全事件启动安全预案，进行止损、分析、定位、制定补救措施、联合相关部门进行溯源和打击。我们亦定期组织内部培训和应急演练，使得我们的相关工作人员掌握相应的应急处置策略和规程。

在不幸发生信息安全事件后，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。**我们同时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，我们还将按照监管部门要求，主动上报信息安全事件的处置情况。

请您理解，由于技术的限制以及风险防范的局限，即便我们已经尽量加强安全措施，也无法始终保证信息百分之百的安全。您接入服务所用的系统和通讯网络，有可能因我们可控范围外的情况而出现问题。

互联网并非绝对安全的环境，而且电子邮件、即时通讯、社交软件或其他服务软件等与其他用户的交流方式无法确定是否完全加密，我们建议您使用此类工具时请使用复杂密码，并注意保护您的信息安全。如果我们的物理、技术，或管理防护设施遭到破坏，导致信息被非授权访问、公开披露、篡改、或毁坏，导致您的合法权益受损，我们将承担相应的法律责任。

请您务必妥善保管好您的账号、密码及其他身份要素。您在使用我们服务时，我们会通过您的账号、密码及其他身份要素来识别您的身份。一旦您泄露了前述信息，您可能会蒙受损失，并可能对您产生不利。如您发现账号、密码及/或其他身份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。

您通过亚数信息平台提交个人信息，代表您同意并授权给亚数信息收集、使用、共享和保护您提供的个人信息，若您因特殊原因申请撤回授权，请及时联系我们，以便于我们做相应处理。

## **六、您的权利**

您可以通过以下方式访问及管理您的个人信息：

### **(一)访问**

您有权访问您的个人信息，法律法规规定的例外情况除外。如果您想行使数据访问权，可以通过以下方式自行访问：

如您希望访问或编辑您的账户中的个人基本信息和更改您的密码、添加认证方式等安全信息，您可以通过登录账号执行此类设置操作。

如果您无法通过上述路径访问这些个人信息，您可通过本文载明的反馈渠道联系我们，在核实您的身份后，我们将向您提供相应信息，但法律法规另有规定的或本政策另有约定的除外。

### **(二)更正或补充您的个人信息**

当您发现我们处理的关于您的个人信息有错误时，您有权要求我们做出更正或补充。您可以通过“（一）访问”中列明的方式提出更正或补充申请。如果

您无法通过上述路径访问这些个人信息，您可通过本文载明的反馈渠道联系我们。

我们将在 30 天内回复您的更正或补充请求。

### **(三)删除您的个人信息**

您可以通过 “（一）访问” 中列明的方式自行删除您的部分个人信息。

在以下情形中，您可以向我们提出删除个人信息的请求：

- 1.如果我们处理个人信息的行为违反法律法规；
- 2.如果我们收集、使用您的个人信息，却未征得您的明确同意；
- 3.如果我们处理个人信息的行为违反了与您的约定；
- 4.如果您不再使用我们的产品或服务，您可主动电话您的客户经理/或通过本文载明的联系方式申请注销账号；
- 5.如果我们不再为您提供产品或服务，但相关法律法规政策另有约定的除外。

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。

当您更正、补充、删除您的个人信息时，我们可能不会立即从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，法律法规另有规定的除外。

### **(四)改变您授权同意的范围**

每个产品、服务或应用需要一些基本的个人信息才能得以完成。对于额外收集的个人信息的收集和使用，您可以随时给予或收回您的授权同意。

您可以通过删除/修改您的个人信息、联系我们或联系与您对接的我们的工作人员来进行操作。

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，不会影响此前给予您的授权而开展的个人信息处理。

### **(五)个人信息主体注销账户**

您随时可注销此前注册的账户，您可以通过以下方式操作：

1. 联系客户经理；
2. 拨打本政策所提供的热线电话。

在注销账户之后，我们将停止为您提供产品或服务，并依据您的要求，删除您的个人信息，法律法规另有规定的除外。

#### **(六)响应您的上述需求**

为保障安全，我们可能会先要求您验证自己的身份，然后再处理您的请求。对于您合理请求，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。

在以下情形中，我们将无法响应您的请求：

- 1.与我们履行法律法规规定的义务相关的；
- 2.与国家安全、国防安全直接相关的；
- 3.与公共安全、公共卫生、重大公共利益直接相关的；
- 4.与刑事侦查、起诉、审判和执行判决等直接相关的；
- 5.我们有充分证据表明您存在主观恶意或滥用权利的；
- 6.出于维护您或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；
- 7.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；
- 8.涉及商业秘密的。

#### **七、第三方服务**

TrustAsia 应用服务中可能接入或链接至第三方提供的服务（包括网站或其他服务形式）或其他类似的应用程序（如嵌入代码、插件等）。

目前，我们接入的第三方服务商主要包括以下几种类型：

- 1.用于消息推送功能，包括站内消息推送、特定事件提醒等；
- 2.用于支付相关服务，包括订单支付、交易行为核验、收入结算、支付信息汇总统计等；
- 3.用于行为验证、接口防刷功能，包括发送短信、发送邮件、密码修改、修改 API 密钥等关键操作的行为验证服务等；



当您在 TrustAsia 中使用第三方提供的服务中，第三方可能会向您收集用户信息。在经您的明示同意后，第三方可能会获取您的姓名、手机号码及其他提供第三方服务所必须的信息；对于您在使用第三方提供的服务时主动提供给第三方的相关信息，我司将视为您允许该第三方获取上述此类信息；对于您在使用该第三方服务时产生的信息，应由您与该第三方依法约定上述信息的收集和使用事项。在将信息提供给第三方前，我司将尽商业上合理的努力评估该第三方收集信息的合法性、正当性、必要性。我司会与第三方签订相关法律文件并要求第三方处理您的个人信息时，遵守法律法规和签署的法律文件，要求第三方对您的信息采取保护措施。如您拒绝第三方在提供服务时收集、使用或者传递上述信息，将可能会导致您无法在 TrustAsia 应用中使用第三方的相应服务，但这不影响您使用 TrustAsia 的其他功能。

第三方推送、支付、行为验证或其他第三方服务，由相关的第三方负责运营。您使用该等第三方服务（包括您向该等第三方提供的任何信息），须受第三方自己的服务条款及信息保护声明（而非本政策）约束，您需要仔细阅读其条款。本政策仅适用于我们所收集的个人信息，并不适用于任何第三方提供的服务或第三方的信息使用规则。如您发现这些第三方服务存在风险时，建议您终止相关操作以保护您的合法权益并及时与我们联系。

## **八、未成年人保护**

我们的产品、网站和服务面向成年人。如果没有父母或监护人的同意，**未满 14 周岁的未成年人不得创建自己的用户账号**。对于经父母或监护人同意处理未满 14 周岁的未成年人个人信息的情况，我们只会在司法机关或行政机关要求、父母或监护人明确同意或者保护未满 14 周岁的未成年人所必要的情况下提供或公开披露此信息。

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未满 14 周岁的未成年人的个人信息，则会设法尽快删除相关数据。

## **九、我们对去世用户的个人信息保护**

我们将根据《中华人民共和国个人信息保护法》等法律法规的规定保护死者个人信息。用户（仅限自然人）去世后，其近亲属为了自身的合法、正当利益，可以通过本隐私政策第十条“联系我们”中公示的联系方式，对去世用户的相关个人信息行使查阅、复制、更正、删除等权利，但是去世用户生前另有安排的除外。

您理解并确认，为了充分保护去世用户的个人信息权益，申请行使本权利的去世用户近亲属需要根据 TrustAsia 的指定流程或客服提示，提交去世用户的身份证明文件、死亡证明文件、申请人的身份证明文件、申请人与去世用户的亲属关系证明文件，并提供申请行使的权利种类、目的。

## 十、您的个人信息如何在全球范围转移

通常情况下，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。

为满足证书申请需要，由于我们的部分产品的最终核验方为境外合作方，这意味着，在获得您的授权同意后，您的个人信息可能会被转移至您购买产品/服务的所在国家/地区的境外管辖区，或者收到来自这些管辖区的访问。

此类管辖区可能设有不同的数据保护法，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个人信息的同意，并根据境内相关法律法规的要求，与境外方签署个人信息出境标准合同等。

**涉及个人信息跨境传输的，您的信息最终将会根据实际产品/服务的类型，传输至下表终端企业。**

企业名称	DPO 联系方式	联系邮箱
Sectigo Limited	+001 2017094352	eric.staudinger@sectigo.com
DigiCert, Inc.	+001 8017019600	dpo@digicert.com
GMO GlobalSign Ltd.	+44 1622766766	dpo@globalsign.com
Asseco Poland S.A.	+48 426756360	daneosobowe@asseccods.pl

## 十一、通知和修订

我们可能会对隐私政策进行修改，并通知您关于隐私政策的更新内容。本政策的任何修改，均将构成本政策的一部分。对于重大变更，我们将通过更为显著的通知向您告知（包括网站公告、推送通知、弹窗提示或其它方式）。如果您不接受修改后的条款，请停止使用我们的服务。我们鼓励您随时查阅本隐私政策，了解我们是如何保护您的个人信息的。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；
- 2.我们在所有权结构方面发生重大变化。如业务调整、破产并购等引起的所有者变更等；
- 3.个人/企业信息共享、转让或公开披露的主要对象发生重大变化；
- 4.您参与个人/企业信息处理方面的权利及其行使方式发生重大变化；
- 5.我们负责处理个人/企业信息安全的责任部门、联络方式及投诉渠道发生重大变化；
- 6.其他重要的或可能严重影响您的个人权益的情况发生。

我们的任何修改都会将您的满意度置于首位。我们鼓励您在每次使用我们服务时都查阅我们的隐私政策。若您在本政策修订后继续使用 TrustAsia 服务，这表示您已充分阅读、理解并接受修订后的本政策并愿意受修订后的本政策约束。

## 十二、如何联系我们

您可通过以下方式与我们联系：

- 1.如您对本政策 内容 有任何疑问、意见或建议，您可通过 电子邮件 [support@trustasia.com](mailto:support@trustasia.com) 或者电话 400-880-8600 与我们联系；
- 2.如发现个人信息可能被泄露，您可以发送邮件到[support@trustasia.com](mailto:support@trustasia.com) 或者通过电话 400-880-8600 投诉举报；

我们将在收到您的问题、意见或建议，并验证您的用户身份后十五个工作日内予以处理。如您不满意我们的处理，您还可以向履行个人信息保护职责的

部门进行投诉、举报。

运营主体名称：亚数信息科技（上海）有限公司

办公地址：上海市徐汇区桂平路 391 号新漕河泾国际商务中心 B 座 32 层

3.我们可能会不时依据法律法规或业务调整对本隐私政策进行修订。

您需理解，只有在您确认并同意变更后的《隐私政策》，我们才会依据变更后的隐私政策收集、使用、处理和存储您的个人信息；您有权拒绝同意变更后的隐私政策，但请您知悉，一旦您拒绝同意变更后的隐私政策，可能导致您不能或不能继续完整使用 TrustAsia 的相关服务和功能，或者无法达到我们拟达到的服务效果。