

# 隐私政策

更新日期：2023 年 7 月 18 日

生效日期：2023 年 7 月 18 日

欢迎使用杭州天谷信息科技有限公司的电子签名服务（以下简称“e 签宝”或“我们”），本隐私政策适用于 e 签宝提供的产品和服务，以及 e 签宝的推广营销行为。

e 签宝尊重并保护您的隐私。我们在处理您提供的信息时将按照本隐私政策收集、存储、使用、传输、提供、公开、删除以及转移您的个人信息。同时，我们通过本隐私政策向您说明，我们为您提供查阅、复制、更正、补充、要求删除这些信息的渠道以及时限。另外，我们通过本隐私政策单独向您说明，我们的 APP 如何处理您的个人信息。

**我们建议您在提供信息给我们之前，务必仔细阅读并了解本隐私政策，特别是加粗部分的条款，在确认充分理解并同意后提供相应的信息，使用我们的产品及服务或与我们建立联系。在本隐私政策更新后继续使用我们的产品和服务、或继续接受 e 签宝的营销推广行为的，意味着您同意本隐私政策（含更新版本）内容，并且同意我们按照本隐私政策处理您的相关信息。如您阅读本协议时全文均未发现加粗、加下划线的条款，则表示您阅读本协议使用的终端存在适配不当的问题，为保障您的权益，建议您在 e 签宝官方网站阅读本协议。**我们更新隐私政策会及时公布于 e 签宝的官方网站，您可以通过 <https://www.esign.cn/gw/fwxy> 查看。除此之外，您还能浏览隐私政策的历史版本及相应的更新生效时间。

**如对本隐私政策内容有任何疑问、意见或建议，或对您提供的任何信息，特别是您的个人信息有具体处理诉求的，您可通过客服电话 400-087-8198 的人工客服通道与我们联系，我们会及时响应并在 15 个工作日内解答您的疑惑、处理您的诉求。**

本隐私政策将帮助您了解以下内容，同时还将帮助您了解 e 签宝 APP 如何处理您的个人信息：

- 一、我们如何收集和使用您的个人信息；
- 二、我们如何存储您的个人信息；
- 三、我们如何共享、转让、公开您的个人信息；
- 四、我们如何保护您的个人信息；
- 五、您在个人信息处理活动中的权利；
- 六、未成年人个人信息保护；
- 七、本隐私政策如何更新。

## 一、我们如何收集和使用您的个人信息

我们根据合法、正当、必要、诚信的原则，收集为实现产品功能或向您提供服务所需要的信息，并将收集信息进行合理利用，我们将尽最大努力确保个人信息处理活动能够保障您的个人信息权益。

我们会在以下情形中收集和使用您的信息，其目的、方式、范围如下：

- （一）注册、登录

您在注册、登录“e 签宝”账户时可以通过第三方平台授权、手机号码或电子邮箱验证码、密码等方式完成。通过第三方平台授权的方式注册、登录的，需要填入您的手机号码或电子邮箱，用以将您的账户与授权第三方平台提供对应账户 ID 及相关信息作关联绑定。通过验证码或密码的方式注册、登录的，需要填入您的手机号码或电子邮箱作为账户登录名。我们使用前述信息为您创建账户，确保您能够在 e 签宝平台登录、使用 e 签宝的服务以及管理您在 e 签宝平台产生的电子数据及信息。

## （二）实名认证

2.1 如您是个人进行实名认证，您需要根据您所选择的实名认证方式，提供您的姓名、人脸识别视频及照片（仅部分认证方式需要收集）、银行卡卡号（仅部分认证方式需要收集）、实名手机号码（仅部分认证方式需要收集）或其他您提供的认证信息。

2.2 如您是企业（含其他类型非自然人）进行实名认证，您需要根据您所选择的实名认证方式，提供您的名称、证件号、法定代表人姓名、法定代表人身份证号码（仅部分认证方式需要收集）、法定代表人实名手机号码（仅部分认证方式需要收集）、对公银行账号信息（仅部分认证方式需要收集）、企业支付宝账号（仅部分认证方式需要收集）或其他您提供的认证信息。

2.3 如您是为企业（含其他类型非自然人）进行实名认证的个人，您需要自行获取企业（含其他类型非自然人）的授权以提供其信息。因您提供的信息造成他人损害的，将由您自行承担。同时，如果该方提出相反意见或者向我们明示不愿受本隐私政策约束的，我们将删除相关信息。

2.4 我们收集实名认证信息是为了满足相关法律法规的实名制要求，若您拒绝，您将无法完成实名认证，亦无法以实名身份签署电子文件。您可以根据自己的意愿选择实名认证的具体方式，实名认证过程中需要提供的信息均会在提交页面中明确告知您，您提交相应的材料即代表您已同意。未实名的 e 签宝账号依然能使用 e 签宝产品的其他基本服务。

## （三）使用 e 签宝服务

3.1 您在使用 e 签宝服务的过程中可根据需要上传电子文件和填写信息。前述数据和信息为您的业务数据，我们将根据您的指令进行操作，包括增加、删除、修改、查询等。

3.2 若您提供他人的个人信息，您需确认获得该方授权且保证该方也知晓并同意受本隐私政策之约束，因您提供的信息造成他人损害的，将由您自行承担。同时，如果该方提出相反意见或者向我们明示不愿受本隐私政策约束的，我们将删除相关信息。

3.3 在获取您明确授权的情况下，我们会通过 e 签宝的合作客户收集您的个人信息，如您授权 e 签宝的合作客户将您的姓名、身份证号、手机号码、邮箱地址、签署完成的电子文件提供给 e 签宝，您可以同时在 e 签宝平台上查看、下载本平台上的信息或文件。我们收集您的前述信息是为了帮助您完成电子签名。

3.4 为了保障我们服务的可用性、连续性及您的账户安全，我们会收集您的下述信息：

3.4.1 设备信息：设备型号、操作系统版本、唯一设备标识符。

3.4.2 软件信息：软件的版本号、浏览器类型。

3.4.3 设备权限：通讯录权限，用于您在签署时便于选择通讯录的联系人作为签署方，并发送相关的签署通知。相机/摄像头权限，用于人脸识别等特定的服务场景。访问照片权限，用于特定服务场景下您自行选择需要上传的保存在您相册内的图片。您可以通过您的设备的应用权限选择开启/关闭上述权限的状态。我们仅能在您主动开启的前提下获得前述权限。

3.4.4 服务日志信息：您在使用我们服务时接入网络的方式、类型和状态、登录时间、操作日志、服务日志等与“e 签宝”服务相关的日志信息。

3.4.5 IP 及位置信息。例如，我们可能会通过 IP 地址、GPS、WiFi 或基站等途径获取您的地理位置信息。您可以选择开启或关闭地理位置信息的授权，如您关闭授权的，与地理位置相

关的功能可能无法使用，可能无法完成相关验证。

3.5 e 签宝 APP 收集的其他个人信息以及获取的权限。当您使用 e 签宝 APP 的时候，APP 需要另行收集的个人信息在本隐私政策末尾“e 签宝 APP 如何处理您的个人信息”单独向您进行说明。

3.6 如您为 e 签盾用户，为了确保后期您的电子文件能更具有证明力，您授权 e 签盾平台收集固定您的签署信息，包括但不限于操作账号的设备信息、网络信息、系统日志、地理位置信息、签署人身份信息、签署方式等数据。

#### （四）COOKIE 技术

在您使用我们的产品或服务时，我们的平台会自动接收并记录您的浏览器和计算机上的信息，其中包括您的 IP 地址、软硬件特征信息、以及您需求的网页记录，COOKIE 中的信息等。为确保网站正常运转，我们会在您的计算机或移动设备上存储名为 Cookie 的小数据文件。在您未拒绝接受 COOKIE 的情况下，COOKIE 将被发送到您的浏览器，并储存在您的计算机硬盘。我们使用 COOKIE 储存您访问我们网站的相关数据，在您访问或再次访问我们的网站时，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。您有权选择接受或拒绝接受 COOKIE。您可以通过修改浏览器的设置以拒绝接受 COOKIE，但是我们需要提醒您，因为您拒绝接受 COOKIE，您将无法使用依赖于 COOKIE 的部分便捷功能。

#### （五）其他情况

5.1 您在申请试用 e 签宝的产品及服务时，我们会通过电话沟通、信息填写等方式收集您的姓名、联系方式、公司名称等信息。我们使用前述信息与您取得联系，为您提供产品试用服务。

5.2 您在接受 e 签宝的推广营销时，我们会通过电话沟通、信息填写等方式收集您的姓名、联系方式、公司名称等信息，根据具体的推广营销内容我们可能会收集您的其他信息以便为您有针对性的推荐我们的产品和服务，但您均可以根据您的意愿决定是否提供给我们。我们使用前述信息向您推荐适合您的 e 签宝产品和服务。

5.3 若您在使用过程中通过我们提供的联系方式联系我们，进行咨询、投诉或产品使用反馈，我们会收集您的信息用以判断您的身份、核实您投诉内容是否真实以及向您告知处理结果。

5.4 本隐私协议列明的内容并不能完整罗列并覆盖未来可能实现的所有功能和业务场景，我们将基于本隐私政策未载明的其他特定目的收集您的信息，但会事先征求您的同意，并不定期更新我们的隐私政策。

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

5.5.1 与我们履行法律法规规定的义务相关的；

5.5.2 与国家安全、国防安全直接相关的；

5.5.3 与公共安全、公共卫生、重大公共利益直接相关的；

5.5.4 与刑事侦查、起诉、审判和判决执行等直接相关的；

5.5.5 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授权同意的；

5.5.6 所收集的个人信息是您自行向社会公众公开的；

5.5.7 为订立、履行个人信息主体作为电子文件一方主体所必需的；

5.5.8 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；

5.5.9 法律、行政法规规定的其他情形。

## 二、 信息存储

（一）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。若为处理跨境业务，确需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、行政

法规和相关监管部门的规定执行。我们会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。

(二) 我们仅在实现 e 签宝服务目所必须的期间和法律法规要求的时限内存储您的个人信息。我们将按照《中华人民共和国网络安全法》的要求，就您使用 e 签宝服务留存相关的网络日志不少于六个月，并根据《电子签名法》及相关法规的规定，保存您的个人信息至少五年，且在保存的时间内依法配合有权机关的查询。在您的个人信息超出保留期间后，除法律法规对于特定信息保留期限另有规定或您与我们达成其他约定外，我们会对您的信息进行删除或做匿名化处理，我们将不会再使用或对外提供您该账户下的个人信息。

(三) 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：

3.1 为遵守适用的法律法规等有关规定；

3.2 为遵守法院判决、裁定或其他生效法律文书的要求；

3.3 为遵守相关政府机关或法定授权组织的要求。

(四) 如我们停止运营“e 签宝”的产品或服务，我们将及时停止处理您个人信息的活动，将停止运营的通知以逐一送达或公告的形式通知您，并对我们存储的个人信息进行删除或匿名化处理。

(五) 您提供的信息在您通过本隐私政策明确的沟通渠道要求我们删除时会由我们会与您联系沟通删除前置事宜。请您理解，“e 签宝”提供的服务为电子签名服务，您所参与签署的电子文件具有法律效力，您的意思表示作出后对依赖方已经产生影响，因此删除您的个人信息需要经过必要的合法性审核并取得依赖方的同意。我们会在收到您的诉求时立即停止使用您的信息，并引导您处理后续事宜。

### 三、我们如何共享、转让、公开您的个人信息

#### (一) 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 我们可能会根据法律法规规定、诉讼争议解决需要，或按有权机关依法提出的强制性要求，对外共享您的个人信息。

1.2 与合作机构共享：为实现电子签名或其他 e 签宝提供的服务的目的，我们的以下服务将由我们和合作机构共同提供。我们会根据法律法规及协议约定与合作机构共享您的某些个人信息。

1.2.1 您的个人身份信息需传输至电子认证服务机构，由电子认证服务机构向您颁发数字证书。使用数字证书是您能够进行电子签名的必要条件，因此如您使用 e 签宝的电子签名服务则需要向 e 签宝合作的电子认证服务机构申请数字证书。您应当自行阅读电子认证服务机构的服务协议，并在同意接受其约束的前提下使用电子签名服务。为保障电子认证服务的有序进行，电子认证服务机构均受到工业和信息化部监管，其服务规则向工业和信息化部备案，按照备案的服务规则向您提供电子认证服务能够保障您的合法权益。

1.2.2 您的个人身份信息需传输至与 e 签宝合作的身份认证服务商，由身份认证服务商提供您在 e 签宝进行身份认证的部分环节的服务。我们会和前述服务商签订数据处理协议，保障其在您授权范围内处理您的个人信息。

1.2.3 您的个人信息及签署电子文件的 hash 值需传输至公证处、司法鉴定中心和蚂蚁区块链，由前述机构提供相应的存证服务及出具相应证明文件。

1.2.4 如您通过第三方服务商平台使用了 e 签宝的服务，为了保证您能够使用第三方服务平台的服务，e 签宝需要将您的个人信息及签署信息共享给第三方服务商。如您为 e 签盾用户，则 e 签盾向您收集的地理位置信息仅作为确认您登录、授权、签章、加密、解密时是否在接收信息一方要求的地理位置范围内之用，该信息由 e 签盾收集并提供给 e 签盾合作的第三

方供应商。

1.2.5 如您在 e 签宝企业空间的角色是“管理员”，为保障您所在企业（含其他类型非自然人）的业务连续性，我们需共享您的部分脱敏个人信息（如：张\*，1\*\*\*\*\*1111），以方便您所在企业的签署相对方或希望加入您所在企业空间的主体顺利与您取得联系。请您知悉，除非得到您的单独授权或在本协议已经明确约定的情形下，e 签宝不会将任何未经脱敏处理的个人信息提供给任何第三方。

1.2.6 e 签宝 APP 通过 SDK 方式共享的信息：APP 需要共享的个人信息在本政策末尾“e 签宝 APP 如何处理您的个人信息”单独向您进行说明。

1.3 向签署依赖方共享您的个人信息。如您使用我们的签署服务签署电子文件，根据电子认证业务规则，我们需要向该份电子文件的签署依赖方共享您的部分个人信息，以证明您作为签署人的真实身份，共享的个人信息包括您通过 e 签宝服务提供的姓名/名称、证件号、数字证书相关信息、实名认证相关信息、签署意愿相关信息以及签署文件相关信息。**如您是企业（含其他类型非自然人）在 e 签宝平台设置的签署用印审批流程节点中对应操作人员，我们也需要向签署依赖方提供您的前述个人信息，以证明您所在企业（含其他类型非自然人）表达签署意愿的真实性。**

1.4 为了让您有更好的体验、改善我们的服务或经您同意的其他用途，在符合相关法律法规的前提下，我们可能将通过某些服务所收集的信息用于我们的其他服务，但我们会进行匿名化处理。例如，将您在使用我们某项服务时的信息，用于用户研究分析与统计等服务。

1.5 为了确保服务的安全，帮助我们更好地了解我们应用程序的运行情况，我们可能记录相关信息或将所收集到的信息用于大数据分析，例如，您应用程序的频率、故障信息、总体使用情况、性能数据或分析形成不包含任何个人信息的城市热力图或行业洞察报告等。我们可能对外公开并与我们的合作伙伴分享经匿名化处理后的信息，用于了解用户如何使用我们服务或让公众了解我们服务的总体使用趋势。

1.6 我们会与共享数据的相对方签订严格的数据处理协议。我们也建议您通过我们合作伙伴的官方网站查阅相应服务的隐私政策。

#### （二）转让

我们不会将您的个人信息转让给其他任何公司、组织和个人，但以下情形除外：

2.1 随着“e 签宝”业务的发展，我们及我们的关联公司有可能进行合并、收购、资产转让或其他类似的交易。如相关交易涉及到您的个人信息转让，我们会要求新持有您个人信息的公司、组织和个人继续受此政策约束，否则我们将要求该公司、组织和个人重新征得您的授权同意。

2.2 在获得您明确同意的情形下转让，我们会向其他方转让我们已经获取的您的个人信息。

#### （三）公开

我们仅会在以下情况下，公开您的个人信息：

3.1 已经获得您明确同意。

3.2 在有权机关强制性要求下，我们可能会公开您的个人信息。

3.3 法律法规规定的其他情形。

### 四、我们如何保护您的个人信息

（一）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访问、公开披露、使用、修改、损坏或丢失。我们会采取一切合理可行的措施，保护您的个人信息。我们使用的技术手段包括但不限于防火墙、TLS/SSL 证书加密传输、去标识化或匿名化处理、访问控制措施等。

（二）我们已经取得了以下认证：ISO/IEC 27701 隐私信息管理体系认证、ISO/IEC 27001 信

息安全管理体系认证、ISO/IEC 27018 公有云个人信息保护管理体系认证、可信云服务认证、公安部信息系统安全等级保护三级认证等国国内外权威认证。我们积极对标国内外信息安全及隐私保护相关的法律法规，通过高强度的认证、高密级的加密保护，不断提升我们的信息安全及隐私保护标准，持续改进我们的产品和服务。

(三)对我们与之共享个人信息的公司、组织和个人，我们会与其签署严格的数据保护条款，要求其按照我们的说明、本隐私政策以及其他任何相关的保密和安全措施来处理个人信息。我们数据安全负责人的联系方式为：sec@tsign.cn。请您知悉，该联系方式不作为接收投诉的渠道。如对本隐私政策内容有任何疑问、意见或建议，或对您提供的任何信息，特别是您的个人信息有具体处理诉求的，您可通过客服电话 400-087-8198 的人工客服通道与我们联系，我们会及时响应并在 15 个工作日内解答您的疑惑、处理您的诉求。

(四)为了保障您的信息安全，我们在收集您的信息后，将采取各种隔离必要的措施保护您的信息。我们会将去标识化后的信息与可用于恢复识别个人的信息分开存储，确保在针对去标识化信息的后续处理中不重新识别个人。我们建立了保障个人信息安全的管理制度、流程和组织。我们要求全体员工签署保密协议，定期开展信息安全、隐私保护系列培训，不断提升员工对信息安全和隐私保护的意识。员工内部系统统一部署 DLP 数据防泄漏系统，对敏感和隐私数据的外发、打印及拷贝进行监控、追踪和审计等。

(五)我们建议您妥善保管您的个人信息，因您个人原因导致账号密码泄露从而导致个人信息泄露的，我们不负责任何责任，但会积极地配合您找回密码或更改密码。

(六)在不幸发生用户信息安全事件（泄露、丢失等）后，我们会启动紧急预案，阻止安全事件扩大。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和可能的影响、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，难以逐一告知用户信息主体时，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，主动上报个人信息安全事件的处置情况。

## 五、您在个人信息处理活动中的权利

### (一) 查阅、复制、更正、补充您的个人信息

您有权管理您的个人信息，法律法规规定的例外情况除外。您可以通过在客户端登录您的 e 签宝账号来查阅、复制、更正、补充您账号中的个人资料信息、更改您的密码、添加安全信息。

如您需要访问其他个人信息，您可以随时通过拨打客服电话 400-087-8198 的人工客服通道与我们联系。我们会及时响应并在 15 个工作日内回复您的请求。

### (二) 删除您的个人信息

您可以通过客服电话 400-087-8198 的人工客服通道来申请删除您的个人信息。

在以下情况发生时，您有权要求“e 签宝”删除您的个人信息：

- 2.1 我们没有征求您的明确同意，收集了您的个人信息；
- 2.2 我们处理您的个人信息违反了法律法规要求；
- 2.3 我们违反了与您的约定处理您的个人信息；
- 2.4 您不再使用我们的产品或服务，或注销了“e 签宝”账号；
- 2.5 我们停止对您提供服务，且已超过约定及法律法规要求的个人信息最低保存期限。

基于业务的需要，为维护交易多方的利益，在本条第二款 2.4 的情形下，我们仍将保留您与实名认证、意愿认证、签署业务直接关联的个人信息。

如您仍想删除此部分信息，需您与依赖方授权同意，我们在收到您与依赖方共同的删除指令后，会将该业务涉及的您的个人信息进行删除。

当您或我们协助您删除相关信息后，因为适用的法律和安全技术，我们可能无法立即从备份系统中删除相应的信息，我们将安全地存储您的个人信息并避免任何进一步处理，直到备份可以清除或实现匿名。

### （三）要求解释说明处理规则

您可以随时通过客服电话 400-087-8198 的人工客服通道与我们取得联系，要求我们解释说明本隐私政策的规则。我们会及时响应并在 15 个工作日内回复您的请求。

### （四）删除您的账号

如您不再使用我们的产品及服务，您有权注销您的账号。

4.1 网页端的注销账号途径为：首页右上角用户头像点击-用户中心-账户设置-注销账号。

4.2 APP 端的注销账号途径在本政策末尾“e 签宝 APP 如何处理您的个人信息”单独向您进行说明。

**请您知悉，因电子签名服务特性，注销账号可能对您已经签署及正在签署的电子文件产生影响，建议您仔细阅读并充分理解《e 签宝服务协议》后，再决定是否注销账号。《e 签宝服务协议》网址：<https://www.esign.cn/gw/fwxy/>。**

## 六、未成年人个人信息保护

**如您是不满 14 周岁的未成年人，应当经过监护人的同意后向我们提供您的个人信息。请您理解，我们提供的服务主要面向成年人，若您是不满 18 周岁的未成年人，在使用我们的产品及相关服务前，应在您监护人监护、指导下共同阅读并同意本隐私政策。**

我们根据国家相关法律法规的规定保护未成年人的个人信息，只会在法律允许、监护人明确同意或保护未成年人所必要的情况下处理未成年人的个人信息；如果我们发现在未事先获得可证实的监护人同意的情况下收集了未成年人的个人信息，则会设法尽快删除相关信息。若您是非成年人的监护人，当您对您所监护的未成年人的个人信息有相关疑问时，您可以随时通过客服电话 400-087-8198 的人工客服通道与我们取得联系。我们会及时响应并在 15 个工作日内回复您的请求。

## 七、本隐私政策如何更新

（一）我们可能适时修订本隐私政策内容。我们会在本页面上发布对本隐私政策所做的任何变更。

（二）对于重大变更，我们还会通过向您的 e 签宝账号发送站内信的方式，告知您最新的隐私政策内容。本隐私政策所指的重大变更包括但不限于：

2.1 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。

2.2 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。

2.3 个人信息共享、转让或公开披露的主要对象发生变化。

2.4 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。

2.5 个人信息安全影响评估报告表明存在高风险时。

（三）如我们的产品和服务业务功能更新后，涉及增加收集个人信息范围的，我们会通过隐私政策更新即时告知您。如您拒绝变更后的隐私政策的，我们将在原有的业务范围内继续为您提供服务，但变更后的隐私政策中存在代替原有业务功能的新增业务功能的信息收集权限的除外。

# e 签宝 APP 如何处理您的个人信息

## 一、基本原则及其他适用条款

e 签宝 APP 处理您的个人信息同样受到本隐私政策约束。因 APP 应用程序的特点，APP 的某些功能可能处理更多您的个人信息，并会通过第三方 SDK 处理您的个人信息。根据相关法律法规的要求，我们在此将 e 签宝 APP 如何处理您的个人信息单独向您进行说明。

## 二、APP 收集的个人信息及用途和必要性

### （一）安卓系统

#### 1.1 注册/登录

收集个人信息类型：手机号码/邮箱

用途及必要性：以手机号/邮箱注册的用户所必须收集的个人信息，用于注册/登录创建账号、完善网络身份标识

#### 1.2 消息推送

收集个人信息类型：去标识化处理后的设备信息（如 IMEI,AndroidId）

用途及必要性：签署、审批功能必须收集的信息，用于签署/审批业务流程节点推送，推送对象为签署人/审批人

#### 1.3 运营与安全保障

收集个人信息类型：设备信息，包括手机型号，系统版本，IMEI，AndroidId，OAID（应用匿名标识），软件版本号，操作，服务日志

用途及必要性：保障用户账户安全（如设备是否属于异常登录）及消息推送

#### 1.4 用户反馈

收集个人信息类型：用户反馈的问题，图片，联系方式（已做相关数据脱敏加密处理）

用途及必要性：联系反馈人、核实反馈问题真实性

### （二）iOS 系统

#### 2.1 注册/登录

收集个人信息类型：手机号码/邮箱

用途及必要性：以手机号/邮箱注册的用户所必须收集的个人信息，用于注册/登录创建账号、完善网络身份标识

#### 2.2 消息推送

收集个人信息类型：去标识化处理后的设备信息（如 UUID，手机型号，系统版本，软件版本号）

用途及必要性：签署、审批功能必须收集的信息，用于签署/审批业务流程节点推送，推送对象为签署人/审批人

#### 2.3 运营与安全保障

收集个人信息类型：设备信息，包括手机型号，系统版本，UUID（应用匿名标识），软件版本号，操作，服务日志

用途及必要性：保障用户账户安全（如设备是否属于异常登录）及消息推送

#### 2.4 用户反馈

收集个人信息类型：用户反馈的问题，图片，联系方式（已做相关数据脱敏加密处理）

用途及必要性：联系反馈人、核实反馈问题真实性



### 三、APP 需要获取的用户权限

#### (一) 安卓系统

##### 1.1 ACCESS\_NETWORK\_STATE

权限功能说明：允许应用检测网络状态

使用场景及目的：请求数据时判断网络是否可以用或者弱网

必要性：基本功能所需权限，APP 需要根据网络状态调整数据的请求和文档的加载

##### 1.2 INTERNET

权限功能说明：允许应用发送数据请求

使用场景及目的：请求服务器数据

必要性：基本功能所需权限，没有网络，您将无法登录账号

##### 1.3 CAMERA

权限功能说明：使用拍摄照片和视频、完成扫描二维码

使用场景及目的：拍照生成文件、录制刷脸认证视频或者扫描二维码打开签署链接

必要性：基本功能所需权限，不授权将无法完成刷脸视频认证业务；无法通过拍照上传文件；无法通过扫码打开签署页面或进行扫码登录业务

##### 1.4 WRITE\_EXTERNAL\_STORAGE

权限功能说明：提供写入外部储存功能

使用场景及目的：允许 APP 写入/下载/保存/修改/删除图片、文件、崩溃日志等信息

必要性：基本功能所需权限，不授权 APP 将无法保存文件到本地，比如下载已经完成签署的文件；保存手机盾数字证书到本地

##### 1.5 READ\_EXTERNAL\_STORAGE

权限功能说明：提供读取手机储存空间内数据的功能

使用场景及目的：允许 APP 读取存储中的图片、文件等内容，主要用于上传文件发起签署，读取在本地记录崩溃日志信息

必要性：基本功能所需权限，不授权 APP 将无法读取本地文件进行上传并发起签署流程；无法读取本地数字证书完成手机盾业务

##### 1.6 READ\_PHONE\_STATE

权限功能说明：提供读取手机设备标识 IMEI 等信息

使用场景及目的：读取设备识别码，识别手机设备 ID，用于消息推送等主要功能和账户安全保障

必要性：基本功能及账户安全保障所需权限，不授权 APP 将无法将签署和审批消息进行推送，无法通过您是否更换手机来确定账号安全

##### 1.7 ACCESS\_WIFI\_STATE

权限功能说明：允许应用获取 MAC 地址和 WIFI 状态

使用场景及目的：根据 MAC 地址和设备识别码生成设备唯一标识，用于消息推送等主要功能和账户安全保障

必要性：基本功能及账户安全保障所需权限，不授权 APP 将无法生成唯一识别码保证消息推送的正确到达，无法提醒用户异地登录等账户异常情况

##### 1.8 READ\_CONTACT

权限功能说明：获取系统中的通信录信息

使用场景及目的：在添加签署人时允许用户导入通信录信息

必要性：基本功能所需权限，不授权此权限，用户将无法将联系人的信息添加为签署人信息发起签署流程

##### 1.9 CALL\_PHONE

权限功能说明：拨打电话

使用场景及目的：允许用户在获取权限后拨打客服电话

必要性：基本功能所需权限，授权用户在 APP 里通过客服电话进行咨询投诉

#### 1.10 USE\_FINGERPRINT

权限功能说明：指纹权限

使用场景及目的：允许读取本地指纹 ID 信息（非指纹信息本身）

必要性：授权后可通过设备存储的指纹识别实现认证签署功能，非必须获取的权限

#### 1.11MANAGE\_FINGERPRINT

权限功能说明：指纹管理权限

使用场景及目的：允许读取本地指纹 ID 信息（非指纹信息本身）

必要性：授权后可通过设备存储的指纹识别实现认证签署功能，非必须获取的权限

#### 1.12 USE\_IFAA\_MANAGER

权限功能说明：IFAA 指纹权限

使用场景及目的：允许读取本地指纹 ID 信息（非指纹信息本身）

必要性：授权后可通过设备存储的指纹识别实现认证签署功能，非必须获取的权限

#### 1.13USE\_FACERECOGNITION

权限功能说明：面容权限

使用场景及目的：允许读取本地面容 ID 信息（非面容信息本身）

必要性：授权后可通过设备存储的面容识别实现认证签署功能，非必须获取的权限

#### 1.14USE\_FACE

权限功能说明：个别厂商面容权限

使用场景及目的：允许读取本地面容 ID 信息（非面容信息本身）

必要性：授权后可通过设备存储的面容识别实现认证签署功能，非必须获取的权限

### （二）iOS 系统

#### 2.1 APP Transport Security Settings - Allow Arbitrary Loads

权限功能说明：允许应用访问 http 协议链接

使用场景及目的：请求网络数据，加载相应网页

必要性：基本功能所需权限，不授权 APP 无法访问 http 链接和 api

#### 2.2 Camera Usage Description

权限功能说明：允许使用相机权限

使用场景及目的：拍照发起签署，用于通过拍摄照片发起签署、使用相机扫描二维码打开链接进行签署、刷脸视频认证功能

必要性：基本功能所需权限。不授权将无法使用拍照发起签署功能；无法扫码签署；无法刷脸视频认证功能

#### 2.3 Microphone Usage Description

权限功能说明：允许使用麦克风权限

使用场景及目的：刷脸视频认证功能

必要性：基本功能所需权限，不授权无法使用刷脸视频认证功能

#### 2.4 Photo Library Additions Usage Description

权限功能说明：允许写入相册权限

使用场景及目的：扫码签保存二维码

必要性：基本功能所需权限，不授权无法保存二维码到相册

#### 2.5 Photo Library Usage Description

权限功能说明：允许读取相册权限

使用场景及目的：从相册发起功能、添加签署文件附件功能

必要性：基本功能所需权限，不授权无法使用从相册发起签署功能；无法从相册添加签署文件以及附件

#### 2.6 NSLocationWhenInUseUsageDescription

权限功能说明：允许使用期间访问地理位置

使用场景及目的：用于获取用户地域分布图，优化用户体验

必要性：优化功能所需，用户可选择性开启

#### 2.7 NSLocationAlwaysUsageDescription

权限功能说明：允许持续访问地理位置

使用场景及目的：用于获取用户地域分布图，优化用户体验

必要性：优化功能所需，用户可选择性开启

#### 2.8 Face ID Usage Description

权限功能说明：Face ID 使用权限

使用场景及目的：用户可以使用存储于本地的面容识别标识确认用户身份完成签署意愿认证

必要性：签署方式多样性功能，用户可选择性开启

### 四、e 签宝 APP 通过 SDK 方式共享的信息

（一）某些产品和服务可能由我们的授权合作机构通过 SDK 的形式向您提供产品或服务。在此过程中，我们的授权合作机构可能会收集、使用和存储您的相关数据或信息，处理您的信息时均通过去标识化、加密传输和处理的安全处理方式。我们列举了具体的授权合作机构，并提供其隐私政策链接，我们建议您阅读其隐私政策。

（二）安卓系统使用的 SDK 服务

#### 2.1 个推 gtc SDK

供应商名称：每日互动股份有限公司

使用目的：推送系统通知及其他消息

必要性：基本功能所需，在签署和审批业务场景中及时将业务流程中的节点信息和结果推送给用户

个人信息类型：设备信息(imei/imsi/iccid/android id/oaid/SN/Mac 地址/系统版本/设备型号/通知开关状态)、网络信息(wifi 相关/ip)

隐私政策链接：<https://docs.getui.com/privacy>

#### 2.2 神策分析 SDK

供应商名称：神策网络科技（北京）有限公司

使用目的：分析用户在 APP 里的行为和业务操作，监测 APP 性能

必要性：不使用则无法分析用户在 APP 里的行为和业务操作保证应用稳定性

个人信息类型：设备信息(imei/imsi/iccid/android id/oaid/SN/Mac 地址/系统版本/设备型号)、网络信息(wifi 相关/ip)

隐私政策链接：[https://www.sensorsdata.cn/market/privacy\\_policy.html](https://www.sensorsdata.cn/market/privacy_policy.html)

#### 2.3 微信分享 SDK

供应商名称：深圳市腾讯计算机系统有限公司

使用目的：使对应微信用户通过微信实现签署、审批、合同查看的基本功能

必要性：把签署业务、审批业务或者签署的文档分享给微信里对应的账号

个人信息类型：设备标识符(IMEI/Mac/AndroidID/IDFA/OPENUDID/GUID、SIM 卡 IMSI 信息)

隐私政策链接：[https://www.wechat.com/zh\\_cn/privacy\\_policy.html](https://www.wechat.com/zh_cn/privacy_policy.html)

#### 2.4 魅族 Flyme 推送 SDK

供应商名称：珠海市魅族通讯设备有限公司

使用目的：推送系统消息及其他消息

必要性：使魅族手机用户收到业务场景中的节点信息推送，如签署链接

个人信息类型：本机设备信息（IMEI、IMSI）、MAC 地址、手机型号、系统类型、系统版本、手机屏幕大小参数

隐私政策链接：<https://i.flyme.cn/privacy>

## 2.5 小米开放平台消息推送 SDK

供应商名称：小米通讯技术有限公司

使用目的：推送系统通知及其他消息

必要性：使小米手机用户收到业务场景中的节点信息推送，如签署链接

个人信息类型：本机设备信息（IMEI、IMSI）、MAC 地址、手机型号、系统类型、系统版本、手机屏幕大小参数

隐私政策链接：[https://privacy.mi.com/all/zh\\_CN](https://privacy.mi.com/all/zh_CN)

## 2.6 OPPO 推送平台 SDK

供应商名称：OPPO 广东移动通信有限公司

使用目的：推送系统通知及其他消息

必要性：使 OPPO 手机用户收到业务场景中的节点信息推送，如签署链接

个人信息类型：本机设备信息（IMEI、IMSI）、MAC 地址、手机型号、系统类型、系统版本、手机屏幕大小参数

隐私政策链接：<https://open.oppomobile.com/wiki/doc#id=10288>

## 2.7 VIVO 消息推送 SDK

供应商名称：维沃移动通信有限公司

使用目的：推送系统通知及其他消息

必要性：使 VIVO 手机用户收到业务场景中的节点信息推送，如签署链接

个人信息类型：本机设备信息（IMEI、IMSI）、MAC 地址、手机型号、系统类型、系统版本、手机屏幕大小参数

隐私政策链接：<https://www.vivo.com.cn/about-vivo/privacy-policy>

## 2.8 华为 APPGallery Connect core SDK/华为 HMS 核心功能 SDK/华为分析服务 SDK/华为消息推送 SDK/华为 Log SDK

供应商名称：华为软件技术有限公司

使用目的：推送系统消息及其他消息

必要性：使华为手机用户收到业务场景中的节点信息推送，如签署链接

个人信息类型：本机设备信息（IMEI、IMSI）、MAC 地址、手机型号、系统类型、系统版本、手机屏幕大小参数

隐私政策链接：<https://developer.huawei.com/consumer/cn/devservice/term/>

## 2.9 腾讯 TBS SDK

供应商名称：深圳市腾讯计算机系统有限公司

使用目的：打开 H5 网页控件，读写本地崩溃信息并进行上报，提高系统兼容性

必要性：如不使用，则部分手机打开 H5 页面会存在兼容性和性能问题

个人信息类型：本机设备信息（IMEI、IMSI）、MAC 地址、手机型号、系统类型、系统版本、手机屏幕大小参数、读写权限

隐私政策链接：<https://x5.tencent.com/docs/privacy.html>

## 2.10 腾讯 Matix Android SDK

供应商名称：深圳市腾讯计算机系统有限公司

使用目的：保障 APP 的稳定性和性能

必要性：提高 APP 性能和稳定性的检测工具

个人信息类型：本机设备信息（IMEI、IMSI）、MAC 地址、手机型号、系统类型、系统版本、手机屏幕大小参数、读写权限

隐私政策链接：<https://x5.tencent.com/docs/privacy.html>

#### 2.11 腾讯 Bugly SDK

供应商名称：深圳市腾讯计算机系统有限公司

使用目的：捕捉 APP 崩溃信息，便于排查和解决线上崩溃问题

必要性：提高 APP 性能和稳定性的检测工具

个人信息类型：日志信息（包括：开发者自定义日志、Logcat 日志以及 APP 崩溃堆栈信息）、设备 ID（包括：androidid）、联网信息、系统名称、系统版本以及国家码

隐私政策链接：<https://bugly.qq.com/v2/contract>

#### 2.12 一砂 SDK

供应商名称：北京一砂信息技术有限公司

使用目的：识别用户身份的信息要素

必要性：通过读取本地生物识别信息，对用户身份进行识别，提高签签署的效率和准确性

个人信息类型：IFAA 设备信息、相机权限、本地生物认证 ID 信息等（不含生物信息本身）

隐私政策链接：<https://edis.esandcloud.com/web/privacy.html>

#### 2.13 电信一键登录 SDK

供应商名称：世纪龙信系网络有限责任公司

使用目的：用户可使用电信账号快速登录

必要性：非必须，用户可不选择使用电信一键登录方式

个人信息类型：运营商、网络状态、设备标识符（如 ICCID）、IP 地址、本机号码、手机设备类型、手机操作系统、硬件厂商

收集方式：SDK 采集

隐私政策链接：<https://e.189.cn/sdk/agreement/detail.do?hidetop=true>

#### 2.14 移动一键登录 SDK

供应商名称：中移互联网有限公司

使用目的：用于提供给用户快速登录账号的能力

必要性：非必须，用户可不选择使用移动一键登录方式

个人信息类型：运营商，网络状态，设备标识符（如 ICCID），IP 地址，本机号码，手机设备类型、手机操作系统、硬件厂商

收集方式：SDK 采集

隐私政策链接：<https://wap.cmpassport.com/resources/html/contract.html>

#### 2.15 联通一键登录 SDK

供应商名称：中国联合网络通信有限公司

使用目的：用于提供给用户快速登录账号的能力

必要性：非必须，用户可不选择使用联通一键登录方式

个人信息类型：运营商，网络状态，设备标识符（如如 ICCID），IP 地址，本机号码，手机设备类型、手机操作系统、硬件厂商、改变网络类型、应用运行列表、网络接入标识

收集方式：SDK 采集

隐私政策链接：<https://opencloud.wostore.cn/authz/resource/html/disclaimer.html>

#### 2.16 应用实时监控服务 App 监控 SDK

供应商名称：阿里云计算有限公司

使用目的：用于崩溃日志的上报及分析

必要性：提高 APP 性能和稳定性的检测工具

个人信息类型：网络信息，设备信息包括操作系统、设备型号、Android 系统设备标识，运营商信息

收集方式：SDK 采集

隐私政策链接：

<https://terms.alicdn.com/legal-agreement/terms/privacy/20220808181437191/20220808181437191.html>

#### 2.17 Zxing 二维码扫描 SDK

供应商名称：谷歌公司

使用目的：二维码扫描

必要性：使用 APP 扫描二维码

个人信息类型：存储信息，设备信息，WIFI 相关信息

收集方式：SDK 采集

隐私政策链接：<https://github.com/zxing/zxing>

#### 2.18 极验行为验证 SDK

供应商名称：武汉极意网络科技有限公司

使用目的及必要性：为用户提供无感本机认证、快捷登录账号

个人信息类型：设备型号、设备制造商、手机系统版本、屏幕尺寸、运营商类型、网络类型、应用名称、应用版本、包名、包签名、ip 地址

所需权限：/

隐私政策链接：<https://www.geetest.com/Private>

#### 2.19 腾讯 MMKV SDK

供应商名称：深圳市腾讯计算机系统有限公司

使用目的及必要性：本地数据存储和读取工具，提高 APP 数据存储和读取性能

个人信息类型：不涉及

所需权限：本地文件信息读写权限

#### 2.20 Facebook fresco SDK

供应商名称：Meta Platforms, Inc.

使用目的及必要性：第三方图片库，提高 APP 加载图片的效率

个人信息类型：不涉及

所需权限：本地文件的读写权限，下载网络图片到本地并读取展示

#### 2.21 Glide SDK

供应商名称：/

使用目的及必要性：第三方图片库，提高 APP 加载图片的效率

个人信息类型：不涉及

所需权限：本地文件的读写权限，下载网络图片到本地并读取展示

#### 2.22 EasyPermissions SDK

供应商名称：谷歌

使用目的及必要性：谷歌提供的 APP 权限获取权限框架

个人信息类型：不涉及

所需权限：/

### （三）iOS 系统使用的 SDK 服务

#### 3.1 个推 gtc SDK

供应商名称：每日互动股份有限公司

使用目的：推送系统通知及其他消息

必要性：基本功能所需，在签署和审批业务场景中及时将业务流程中的节点信息和结果推送给用户

个人信息类型：设备信息(mac 地址/idfa/设备型号/deviceToken/allowNotification 通知状态)、网络信息(wifi 相关/ip)

隐私政策链接：<https://docs.getui.com/privacy>

#### 3.2 神策分析 SDK

供应商名称：神策网络科技（北京）有限公司

使用目的：分析用户在 APP 里的行为和业务操作，监测 APP 性能

必要性：不使用则无法分析用户在 APP 里的行为和业务操作保证应用稳定性

个人信息类型：设备信息(mac 地址/idfa/设备型号/屏幕宽高)、网络信息(wifi 相关/ip)

隐私政策链接：[https://www.sensorsdata.cn/market/privacy\\_policy.html](https://www.sensorsdata.cn/market/privacy_policy.html)

#### 3.3 UMConfigure

供应商名称：北京锐讯灵通科技有限公司

使用目的：用于用户数据统计、app 崩溃优化、app 微信分享、app 优化分析

必要性：基本功能所需，如不使用无法进行 app 优化分析

个人信息类型：设备 Mac 地址、唯一设备识别码

隐私政策链接：<https://www.umeng.com/policy>

#### 3.4 电信一键登录 SDK

供应商名称：世纪龙信系网络有限责任公司

使用目的：用户可使用电信账号快速登录

必要性：非必须，用户可不选择使用电信一键登录方式

个人信息类型：运营商、网络状态、设备标识符（如 ICCID）、IP 地址、本机号码、手机设备类型、手机操作系统、硬件厂商

隐私政策链接：<https://e.189.cn/sdk/agreement/detail.do?hidetop=true>

#### 3.5 移动一键登录 SDK

供应商名称：中移互联网有限公司

使用目的：用于提供给用户快速登录账号的能力

必要性：非必须，用户可不选择使用移动一键登录方式

个人信息类型：运营商，网络状态，设备标识符（如 ICCID），IP 地址，本机号码，手机设备类型、手机操作系统、硬件厂商

收集方式：SDK 采集

隐私政策链接：<https://wap.cmpassport.com/resources/html/contract.html>

#### 3.6 联通一键登录 SDK

供应商名称：中国联合网络通信有限公司

使用目的：用于提供给用户快速登录账号的能力

必要性：非必须，用户可不选择使用联通一键登录方式

个人信息类型：运营商，网络状态，设备标识符（如如 ICCID），IP 地址，本机号码，手机设备类型、手机操作系统、硬件厂商、改变网络类型、应用运行列表、网络接入标识

收集方式：SDK 采集

隐私政策链接：<https://opencloud.wostore.cn/authz/resource/html/disclaimer.html>

### 3.7 应用实时监控服务 App 监控 SDK

供应商名称： 阿里云计算有限公司

使用目的： 用于崩溃日志的上报及分析

必要性： 提高 APP 性能和稳定性的检测工具

个人信息类型： 网络信息，设备信息包括操作系统、设备型号、Android 系统设备标识，运营商信息

收集方式： SDK 采集

隐私政策链接：

<https://terms.alicdn.com/legal-agreement/terms/privacy/20220808181437191/20220808181437191.html>

### 3.8 极验行为验证 SDK

供应商名称： 武汉极意网络科技有限公司

使用目的及必要性： 提供验证码行为验证服务，降低 APP 被机器破解的概率

个人信息类型： 不涉及

所需权限： /

隐私政策链接： <https://www.geetest.com/Private>

### 3.9 AFHTTPSessionManager

供应商名称： /

使用目的： 用于实现网络请求

必要性： 基本功能所需，如不使用则 APP 无法与服务器进行有效交互

个人信息类型： 本机设备信息（IMEI、IMSI）、2.MAC 地址、手机型号、系统类型、系统版本、手机屏幕大小参数；检测网络状态

隐私政策链接： /

### 3.10SDWebImageManager

供应商名称： /

使用目的及必要性： 实现扫一扫功能，基本功能所需，不使用无法扫描二维码

个人信息类型： 不涉及

所需权限： 摄像头权限

### 3.11 SDCycleScrollView

供应商名称： /

使用目的及必要性： 用于 banner 轮播功能的实现

个人信息类型： 不涉及

所需权限： /

### 3.12 Reachability

供应商名称： /

使用目的及必要性： 用于检测 APP 网络状态

个人信息类型： 不涉及

所需权限：

### 3.13MJRefresh

供应商名称： /

使用目的及必要性： 用于检测 APP 网络状态

个人信息类型： 不涉及

所需权限： /

### 3.14 MBProgressHUD



供应商名称： /

使用目的及必要性： 用于实现 toast/dialog 等交互弹窗

个人信息类型： 不涉及

所需权限： /

### 3.15 MASConstraintMaker

供应商名称： /

使用目的及必要性： 用于页面布局

个人信息类型： 不涉及

所需权限： /

### 3.16 CJSONSerializer

供应商名称： /

使用目的及必要性： 用于提供 json 数据解析能力

个人信息类型： 不涉及

所需权限： /

## （四）其他

4.1 当 APP 在后台运行时，提供消息推送及性能监控和日志上传服务的 SDK 会继续运行。这是为了保证业务推送消息的可达性，推送服务需要在后台继续运行，包括个推 SDK 和用户手机厂商对应的提供消息推送服务的 SDK；为了保证 APP 的兼容性和稳定性，会在 APP 空闲或后台空闲时上传日志，进行性能和错误分析，包括神策分析 SDK、腾讯 Bugly SDK、腾讯 TBS SDK。

4.2 请您知悉，我们仅会出于合法、正当、必要的目的共享您的个人信息，并且只会共享提供服务所必要的个人信息。我们会对授权合作机构开展个人信息安全影响评估，对其收集的个人信息或需要授权获得的权限进行合理性分析，定期对其服务能力和安全能力进行评估和监控，并与其签订有关协议明确约定严格的数据保护措施，要求其应遵守相关的法律法规的规定，严格按照我们的标准、本隐私政策以及其他任何相关的保密和安全措施来处理您的个人信息。以上 SDK 合作机构均通过去标识化、加密传输和处理的安全处理方式处理您的个人信息。

4.3 如您在使用过程中一旦发现我们的授权合作机构有违法违规的行为，您可以随时通过拨打客服电话 400-087-8198 的人工客服通道与我们取得联系。我们会予以核实并及时中止与该第三方的合作，尽最大可能保障您的个人数据和隐私信息不受侵害。

## 五、其他

如您不再使用我们的产品及服务，您有权注销您的账号，APP 的注销账号途径为：首页我的-账户安全-注销账号。