

用户隐私政策

更新日期：2021 年 11 月 23 日

生效日期：2021 年 11 月 23 日

欢迎访问杭州天谷信息科技有限公司的电子签名平台（以下简称“e 签宝”或“我们”），本隐私政策适用于我们提供的产品和服务，包括电子签名产品、存证服务、法律服务等。

我们尊重并保护您的隐私。您在使用“e 签宝”的服务时，我们将按照本隐私政策收集、使用、存储、共享、转让、公开披露、删除您的个人信息。同时，我们会通过本隐私政策向您说明，我们如何为您提供的访问、更改、删除和保护这些信息的方式。我们建议您在“e 签宝”服务前，务必仔细阅读并了解本隐私政策，在确认充分理解并同意后使用我们的产品或服务。在您使用或在我们更新本隐私政策后继续使用“e 签宝”的产品或服务，即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收集、使用、存储、分享、转让、公开披露和删除您的相关信息。如对本隐私政策内容有任何疑问、意见或建议，您可通过本隐私政策提供的各种联系方式与我们联系。

本隐私政策将帮助您了解以下内容：

- 一、我们如何收集您的个人信息；
- 二、我们如何使用您的个人信息；
- 三、我们如何共享、转让、公开披露您的个人信息；
- 四、我们如何使用 COOKIES 技术；
- 五、我们如何存储您的个人信息；
- 六、我们如何保护您的个人信息；
- 七、您管理个人信息的权利；
- 八、未成年人个人信息保护；
- 九、免责声明；
- 十、本隐私政策如何更新；
- 十一、如何联系我们。

一、我们如何收集您的个人信息

我们根据合法、正当、必要的原则，收集为实现产品功能所需要的信息，并将收集信息进行合理使用。

我们会收集以下个人或企业信息：

（一）您在注册、实名认证时提供的信息

1.1 您在注册“e 签宝”账户时需要提供手机号码或电子邮箱作为账户登录名。如您不提供前述信息，您将无法注册“e 签宝”账户或无法使用“e 签宝”的服务（通过第三方平台登录的情况可能不需要提供手机号码或电子邮箱，具体以第三方平台与我们的约定为准，您可以通过本协议所载明的各种联系方式联系我们进行咨询）。

1.2 如您选择进行实名认证服务，您需要根据您所选择的实名认证方式，提供您的真实姓名、身份证/护照等身份证明、人脸识别视频、面部照片、银行卡信息、手机号码、个人手写签

名或其他您提供的认证信息。收集此类信息是为了满足相关法律法规的实名制要求，若您不提供此类信息，您将无法完成实名认证，亦无法以实名身份签发文件。

如您是法人单位，我们还可能会收集您的公司营业执照信息或组织机构代码证信息、法定代表人姓名及有效证件号码或者身份证正反面照片、公司住所地、公司电话号码或公司对公银行账户信息。

（二）您在使用过程中提供的信息

我们会收集您主动上传至我们的材料，包含合同原文、哈希值或其他书面材料，该文件或材料可能涉及您的隐私信息或商业秘密。我们会对上述信息进行安全保存。除非您主动提交合同审阅的服务，我们不会主动收集或分析这些信息。

若您提供的是他人的信息，包括姓名、电话号码、身份证号、收件地址、邮箱地址等个人隐私信息，您需确认获得对方授权且保证对方也知晓并同意受本隐私协议之约束，因您提供的信息造成他人损害的，将由您自行承担责任。同时，如果他人提出相反意见或者向我们明示不愿受本隐私协议约束的，我们将删除相关信息。

此外，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：

- 2.1 设备信息：**设备型号、操作系统版本、唯一设备标识符、IP 地址信息。
- 2.2 软件信息：**软件的版本号、浏览器类型。为确保操作环境的安全或提供服务所需（调用其他 APP 用于认证服务），我们会收集有关您使用的移动应用和其他软件的信息。
- 2.3 某些设备权限：**我们可能基于您的允许获得某些设备权限，包括通讯录权限，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。我们不会保存您的通讯录信息作为他用；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。
- 请您知悉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。我们仅能在您允许/开启通讯录、相机/摄像头、访问照片的权限的前提下获得上述权限。
- 2.4 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。
- 2.5 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。
- 2.6 e 签宝 APP 收集的个人信息以及获取的权限。**

APP 收集的个人信息及用途和必要性包括：

Android		
业务模块	收集的个人信息类型	收集个人信息的用途及必要性
注册/登录	手机号码	以手机号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
消息推送	去标识化处理后的设备信息（如IMEI,AndroidId）	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
运营与安全保障	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	保障用户账户安全（如设备是否属于异常登录）及消息推送
用户反馈	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）	用户反馈问题时，可能上传的图片，或联系方式（邮箱，qq，微信或手机号）

IOS		
业务模块	收集的个人信息类型	收集个人信息的用途及必要性
注册/登录	手机号码	以手机号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
消息推送	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）	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
运营与安全保障	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	保障用户账户安全（如设备是否属于异常登录）及消息推送
用户反馈	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）	用户反馈问题时，可能上传的图片，或联系方式（邮箱，qq，微信或手机号）

APP 基于基本功能实现以及账户安全保障的需要，需要获取用户的以下权限：

Android			
权限名称	权限功能说明	使用场景及目的	必要性
ACCESS_NETWORK_STATE	允许应用检测网络状态	请求数据时判断网络是否可以用或者弱网	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
INTERNET	允许应用发送数据请求	请求服务器数据	基本功能所需权限，没有网络，您将无法登录账号
CAMERA	使用拍摄照片和视频、完成扫描二维码	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	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
WRITE_EXTERNAL_STORAGE	提供写入外部储存功能	允许 App 写入/下载/保存/修改/删除图片、文件、崩溃日志等信息	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
READ_EXTERNAL_STORAGE	提供读取手机储存空间内数据的功能	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	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
READ_PHONE_STATE	提供读取手机设备标识 IMEI 等信息	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	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
ACCESS_WIFI_STATE	允许应用获取 MAC 地址和 WIFI 状态	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	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

		保障	情况
READ_CONTACT	获取系统中的通信录信息	在添加签署人时允许用户导入通信录信息	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
CALL_PHONE	拨打电话	允许用户在获取权限后拨打客服电话	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
IOS			
权限名称	权限功能说明	使用场景及目的	必要性
App Transport Security Settings - Allow Arbitrary Loads	允许应用访问http协议链接	请求网络数据，加载相应网页	基本功能所需权限，不授权APP无法访问http链接和api
Camera Usage Description	允许使用相机权限	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	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
Microphone Usage Description	允许使用麦克风权限	刷脸视频认证功能	基本功能所需权限，不授权无法使用刷脸视频认证功能
Photo Library Additions Usage Description	允许写入相册权限	扫码签保存二维码	基本功能所需权限，不授权无法保存二维码到相册
Photo Library Usage Description	允许读取相册权限	从相册发起功能、添加签署文件附件功能	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

（三）第三方为实现签约目的提供给我们的信息

在获取您明确同意的情况下，我们会与e签宝的合作客户共享您的个人信息，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共享至e签宝平台，您可以在本平台上查看、下载本平台上的信息或文件。

（四）其他信息

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。

（五）征得授权同意的例外

根据相关法律法规规定，以下情形中收集您的个人信息无需征得您的授权同意：

- 5.1 与个人信息控制者履行法律法规规定的义务相关的；
- 5.2 与国家安全、国防安全直接相关的；

- 5.3 与公共安全、公共卫生、重大公共利益直接相关的；
- 5.4 与刑事侦查、起诉、审判和判决执行等直接相关的；
- 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您本人授权同意的；
- 5.6 所收集的个人信息是您自行向社会公众公开的；
- 5.7 根据个人信息主体要求签订和履行合同所必需的；
- 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；
- 5.9 根据您的要求签订合同所必需的或双方已在合同中另行约定的；
- 5.10 用于维护所提供的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；
- 5.11 学术研究机构基于公共利益开展统计或学术研究所必要，且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。

二、我们如何使用您的个人信息

我们将严格遵守法律法规及与您的约定，将收集到的信息进行如下使用：

- （一）帮助您注册成为我们的用户；
- （二）向您提供产品和服务，包括依托第三方完成的实名认证、意愿认证、存证等服务的合理使用；
- （三）产品开发和优化；
- （四）为了让您更方便的查看合同，授权支付宝合同管家小程序提供您已签署合同的查看等功能；
- （五）其他用途：当我们要将信息用于本隐私政策未载明的其他用途或要将基于特定目的收集的信息用于其他目的时，会事先征求您的同意。

您的信息将会存储在 e 签宝的服务器上。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。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，但我们不会将我们存储在分析软件中的信息与您在应用程序中提供的个人身份信息相结合。

三、我们如何共享、转让、公开披露您的个人信息

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：

- （一）共享
 - 1.1 我们可能会根据法律法规规定、诉讼争议解决需要，或按行政、司法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，我们的某些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伙伴共享您的某些个人信息。
 - （1）您的个人身份信息及签署信息需传输至电子认证服务机构(简称 CA，Certificate Authority)、公证处、司法鉴定中心、区块链、互联网法院、仲裁委、第三方身份认证机构，由上述权威机构出具相应证明文件或基于处理案件的目的进行使用并保存。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。

(2) e 签宝 APP 通过 SDK 方式共享的信息：某些产品和服务可能由我们的授权合作机构提供，我们会通过 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，我们列举了具体的授权合作机构，并提供了该第三方的隐私政策链接，我们建议您阅读该第三方的隐私政策。

APP 集成的涉及收集个人信息或相关数据的第三方 SDK 及其目的、方式和范围：

Android						
SDK 名称	第三方名称	使用目的	必要性	处理方式	个人信息类型	第三方隐私政策链接
个推 gtc SDK	每日互动股份有限公司	推送系统通知及其他消息	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	通过去标识化、加密传输和处理的安全处理方式	1、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)；2、网络信息(wifi 相关/ip)	https://docs.getui.com/privacy/
神策分析 SDK	神策网络科技有限公司(北京)有限公司	分析用户在 APP 里的行为和业务操作，监测 APP 性能	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	通过去标识化、加密传输和处理的安全处理方式	1、设备信息(imei/imsi/iccid/android id/oaid/SN/Mac 地址/系统版本/设备型号)；2、网络信息(wifi 相关/ip)	https://www.sensorsdata.cn/market/privacy_policy.html
微信分享 SDK	深圳市腾讯计算机系统有限公司	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	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	通过去标识化、加密传输和处理的安全处理方式	设备标识符(IMEI/Mac/Android ID/IDFA/OPENUD ID/GUID、SIM 卡 IMSI 信息)	https://www.wechat.com/zh_cn/privacy_policy.html
魅族 Flyme 推送 SDK	珠海市魅族通讯设备有限公司	推送系统消息及其他消息	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	通过去标识化、加密传输和处理的安全处理方式	本机设备信息(IMEI、IMSI)；2.MAC 地址；3.手机型号、系统类型、系统版本、手机屏幕大小参数	https://i.flyme.cn/privacy

小米开放平台消息推送 SDK	小米通讯技术有限公司	推送系统通知及其他消息	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	通过去标识化、加密传输和处理的安全处理方式	本机设备信息 (IMEI、IMSI) ; MAC 地址 ; 3.手机型号、系统类型、系统版本、手机屏幕大小参数	https://privacy.mi.com/all/zh_CN/
OPPO 推送平台 SDK	OPPO 广东移动通信有限公司	推送系统通知及其他消息	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	通过去标识化、加密传输和处理的安全处理方式	本机设备信息 (IMEI、IMSI) 2.MAC 地址 ; 3.手机型号、系统类型、系统版本、手机屏幕大小参数	https://open.oppomobile.com/wiki/doc#id=10288
VIVO 消息推送 SDK	维沃移动通信有限公司	推送系统通知及其他消息	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	通过去标识化、加密传输和处理的安全处理方式	本机设备信息 (IMEI、IMSI) ; MAC 地址; 3.手机型号、系统类型、系统版本、手机屏幕大小参数	https://www.vivo.com.cn/about-vivo/privacy-policy
华为 SDK※	华为技术有限公司	推送系统消息及其他消息	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	通过去标识化、加密传输和处理的安全处理方式	1.本机设备信息 (IMEI、IMSI) ; 2.MAC 地址; 3.手机型号、系统类型、系统版本、手机屏幕大小参数	https://developer.huawei.com/consumer/cn/devservice/terms/
腾讯 TBS SDK	深圳市腾讯计算机系统有限公司	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	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	通过去标识化、加密传输和处理的安全处理方式	本机设备信息 (IMEI、IMSI) ; 2.MAC 地址; 3.手机型号、系统类型、系统版本、手机屏幕大小参数; 4.读写权限	《腾讯浏览服务 SDK 隐私保护声明》 https://x5.tencent.com/docs/privacy.html
腾讯	深圳	保障 App	提高 App 性	通过去	本机设备信息	https://x5.tencent.com/docs/privacy.html

Matix Android SDK	市腾讯计算机系统有限公司	的稳定性和性能	能和稳定性的检测工具	标识化、加密传输和处理的安全处理方式。	(IMEI、IMSI) ; 2.MAC 地址; 3.手机型号、系统类型、系统版本、手机屏幕大小参数; 4.读写权限	ent.com/docs/privacy.html
腾讯 Bugly SDK	深圳市腾讯计算机系统有限公司	捕捉 APP 崩溃信息, 便于排查和解决线上崩溃问题	提高 App 性能和稳定性的检测工具	通过去标识化、加密传输和处理的安全处理方式	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	https://bugly.qq.com/v2/contract
※华为 SDK 包括: 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						
IOS						
SDK 名称	第三方名称	使用目的	必要性	处理方式	个人信息类型	第三方隐私政策链接
个推 gtc SDK	每日互动股份有限公司	推送系统通知及其他消息	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	通过去标识化、加密传输和处理的安全处理方式	1、设备信息(mac 地址/idfa/设备型号/deviceToken/allowNotification 通知状态) ; 2、网络信息(wifi 相关/ip)	https://docs.getui.com/privacy/
神策分析 SDK	神策网络科技有限公司 (北京) 有限公司	分析用户在 APP 里的行为和业务操作, 监测 APP 性能	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	通过去标识化、加密传输和处理的安全处理方式	1、设备信息(mac 地址/idfa/设备型号/屏幕宽高); 2、网络信息(wifi 相关/ip)	https://www.sensorsdata.cn/market/privacy_policy.html
UMConfi	北京	用于用户	基本功能所	通过去	1.设备 Mac 地址;	https://www.u

gure	锐讯 灵通 科技 有限 公司	数据统计、 app 崩溃优 化、app 微 信分享、 app 优化分 析	需，如不使用 无法进行 app 优化分析	标识 化、加 密传 输和 处 理 的 安 全 处 理 方 式	2.唯一设备识别 码	meng.com/poli cy
AFHTTPS essionM anager	无	用于实现 网络请求	基本功能所 需，如不使用 则 App 无法 与服务器进 行有效交互	通过去标 识化、加 密传 输和 处 理 的 安 全 处 理 方 式	本机设备信息 (IMEI、IMSI)； 2.MAC 地址； 3.手机型号、系统 类型、系统版本、 手机屏幕大小参 数； 4.检测网络状态	

APP 集成的不涉及收集个人信息或相关数据的第三方 SDK 及其目的和需要获取的权限：

Android				
SDK 名称	第三方名称	使用目的及必要性	处理方式	所需权限
腾讯 MMKV SDK	深圳市腾讯计 算机系统有限 公司	本地数据存储和读 取工具，提高 APP 数 据存储和读取性能	通过去标识化、 加密传输和处理 的安全处理方式	本地文件信息读写 权限
极验行为 验证 SDK	武汉极意网络 科技有限公司	提供验证码行为验 证服务，降低 APP 被 机器破解的概率	通过去标识化、 加密传输和处理 的安全处理方式	无
Facebook fresco SDK	Facebook	第三方图片库，提高 APP 加载图片的效率	通过去标识化、 加密传输和处理 的安全处理方式	本地文件的读写权 限，下载网络图片到 本地并读取展示
Glide SDK	无	第三方图片库，提高 APP 加载图片的效率	通过去标识化、 加密传输和处理 的安全处理方式	本地文件的读写权 限，下载网络图片到 本地并读取展示
EasyPerm issions SDK	谷歌	谷歌提供的 APP 权限 获取权限框架	通过去标识化、 加密传输和处理 的安全处理方式	无
IOS				
SDK 名称	第三方名称	使用目的及必要性	处理方式	所需权限
极验行为 验证 SDK	武汉极意网络 科技有限公司	提供验证码行为验 证服务，降低 APP 被	通过去标识化、 加密传输和处理	无

		机器破解的概率	的安全处理方式	
SDWebImageManager	无	实现扫一扫功能，基本功能所需，不使用无法扫描二维码	通过去标识化、加密传输和处理的安全处理方式	摄像头权限
SDWebImageManager	无	实现图片异步加载功能	通过去标识化、加密传输和处理的安全处理方式	无
SDCycleScrollView	无	用于 banner 轮播功能的实现	通过去标识化、加密传输和处理的安全处理方式	无
Reachability	无	用于检测 APP 网络状态	通过去标识化、加密传输和处理的安全处理方式	无
MJRefresh	无	用于实现列表刷新功能	通过去标识化、加密传输和处理的安全处理方式	无
MBProgressHUD	无	用于实现 toast/dialog 等交互弹窗	通过去标识化、加密传输和处理的安全处理方式	无
MASConstraintMaker	无	用于页面布局	通过去标识化、加密传输和处理的安全处理方式	无
CJSONSerializer	无	用于提供 json 数据解析能力	通过去标识化、加密传输和处理的安全处理方式	无

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。这是因为：1、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。2、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。

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。

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，您可以通过本隐私政策提供的联系方式与我们取得联系，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。

1.3 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。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。

1.4 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统计加工后不含身份识别内容的信息，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。

（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）公开披露

我们仅会在以下情况下，公开披露您的个人信息：

3.1 已经获得您明确同意。

3.2 在法律、法律程序、诉讼或政府主管部门强制性要求的情况下，我们可能会公开披露您的个人信息。

3.3 法律法规规定的其他情形。

四、 我们如何使用 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，您生成的电子签章，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，您可能无法使用依赖于 COOKIE 的部分功能。

五、 我们如何存储您的个人信息

（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）我们仅在本隐私政策所属目的所必须期间和法律法规要求的时限内存储您的个人信息，根据《电子签名法》规定，我们会保存您的个人信息至少五年。

（三）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：

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、裁定或其他法律程序的规定；
- 3.3 为遵守相关政府机关或法定授权组织的要求；
- 3.4 我们有理由确信需要遵守法律法规等有关规定；
- 3.5 为执行相关服务协议或本隐私政策、维护社会公共利益，为保护我们的客户、我们或我们的关联公司、其他用户或雇员的人身财产安全或其他合法权益所合理必需的用途。

（四）如我们停止运营“e 签宝”的产品或服务，我们将及时停止继续收集您个人信息的活动，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。

六、 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。我们的应用服务全站使用 **https** 传输协议，采用权威 **CA** 颁发的 **TLS/SSL** 证书加密传输，确保您的个人信息和数据在传输过程中的机密性和完整性。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。

（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认证、可信云服务认证、公安部信息安全等级保护三级认证等国际及国内权威认证。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）我们承诺我们将使信息安全保护达到业界领先的安全水平。为保障您的信息安全，我们致力于使用各种安全技术及配套的管理体系来尽量降低您的信息被泄露、毁损、误用、非授权访问、非授权披露和更改的风险。例如：通过网络安全软件（**SSL**）进行安全传输、信息安全存储、严格限制数据中心的访问。传输和存储个人敏感信息（含个人生物识别信息）时，我们将采用安全、权限控制、去标识化等安全措施。同时我们对数据采取了备份和恢复技术，在数据丢失的情况下及时恢复。

（四）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。

（五）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。

（六）在不幸发生用户信息安全事件（泄露、丢失等）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 and 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。

七、 您管理个人信息的权利

（一）访问您的个人信息

您有权访问您的个人信息，法律法规规定的例外情况除外。您可以通过访问 www.esign.cn 来查询、编辑您账号中的个人资料信息、更改您的密码、添加安全信息。

如您无法通过上述方式访问个人信息，您可以随时通过拨打客服电话 400-087-8198 或 0571-85785223 与我们联系。

我们将在 15 天内回复您的访问请求。

（二）删除您的个人信息

您可以通过拨打客服电话 400-087-8198 或 0571-85785223 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来使用和处理您的个人信息。

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。

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，需您与业务全部相关方授权同意，我们在收到您与业务全部相关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）更正您的个人信息

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。您可以通过 www.esign.cn 或联系客服予以更正。

如您无法通过上述方式更正您的个人信息，您可以随时通过拨打客服电话 400-087-8198 或 0571-85785223 与我们联系，我们将在 15 天内回复您的访问请求。

（四）注销

如您不再需要使用我们的产品或服务，您可以通过 www.esign.cn 申请注销您的账户，我们承诺在 15 天内完成核查和处理。

请您知悉，如您注销“e 签宝”账户后，您将无法再以此账号登录和使用我们的产品和服务，我们将终止为该账号提供电子签名产品服务、存证服务、法律服务等。账号注销完成将无法恢复。但我们善意地提示您，为符合相关法律法规地要求，您在使用我们的产品和服务期间提供或产生地个人信息和数据我们仍会根据《电子签名法》的要求保存至少五年。

八、 未成年人个人信息保护

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，应在您的父母或其他监护人监护、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、父母或其他监护人明确同意或保护未成年人所必要的情况下收集、使用、共享或披露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父母或其他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，当您对您所监护的非成年人的个人信息有相关疑问时，请通过本隐私政策公示的联系方式与我们联系。

九、 免责声明

（一）“e 签宝”含有其他网站的链接，我们可能在任何需要的时候增加商业伙伴或共用品牌的网站。“e 签宝”对您通过“e 签宝”链接到其他网站需要的隐私保护不负任何责任。

（二）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，“e 签宝”不负任何责任，但我们会积极地配合您找回密码或更改密码。

十、 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，我们还会提供更为显著的通知（我们会通过电子邮件或在浏览页面做显著提示的方式，说明本隐私政策的具体变更内容）。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（包括 APP）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。

十一、 如何联系我们

如果您对我们的隐私政策及对您个人信息的处理有任何疑问、意见、建议或投诉，可通过客服电话 400-087-8198 或 0571-85785223 来反馈，我们提供 7*24 小时的热线服务。