移动应用安全监测/移动威胁感知隐私政策

隐私政策更新（日期：2023 年 4 月 12 日）

北京梆梆安全科技有限公司（以下统称“梆梆安全”）承诺将按法律法规要求，采用相应安全保护措施，保护使用梆梆安全“移动应用安全监测/移动威胁感知”产品及其服务（以下统称“安全监测”或“安全监测服务”）之用户（以下统称“用户”或“您”）的个人信息和隐私安全。您在使用安全监测时，梆梆安全可能会收集和使用您的相关个人信息。梆梆安全希望通过《移动安全监测 SDK 隐私政策》（以下简称“本隐私政策”）向您说明梆梆安全在收集和使用您相关个人信息时对应的处理规则等相关事宜，以便更好地保障您的权益。

移动应用安全监测平台是一款为移动应用开发者（以下简称“开发者”）提供应用运行时安全监测的产品，开发者在其移动应用内集成安全监测 SDK 后，可通过采集设备相关信息来用于判断当前 App 所运行的手机设备的安全性，防止恶意的用户对 App 进行网络安全攻击，保护用户的财产安全。开发者在其移动应用集成并使用安全监测 SDK 服务时，委托安全监测 SDK 处理开发者移动应用相关数据信息，其中可能包括开发者移动应用最终用户（以下简称“最终用户”）的个人信息。此隐私政策旨在帮助开发者及最终用户了解我们收集最终用户个人信息的类型及我们如何利用和保护最终用户的个人信息。

特别说明：

1、如果开发者在其移动应用中集成并使用安全监测 SDK 服务，则开发者应承诺：

（1）开发者应遵守收集、使用最终用户个人信息有关的所有可适用法律、政策和法规，保护用户个人信息安全。

（2）开发者应将在其移动应用中集成并使用安全监测 SDK 服务的情况，以及安全监测 SDK 对最终用户必要个人信息的收集、使用和保护规则（即本隐私政策），在其移动应用的显著位置或以其他可触达最终用户的方式告知最终用户（包括但不限于：在其移动应用隐私政策显眼处提供最终用户可浏览本隐私政策的链接），并获得最终用户对于安全监测 SDK 收集、使用最终用户相关个人信息的完整、合法、在使用安全监测 SDK 服务期间持续有效的授权同意。如果开发者的移动应用最终用户是未满 14 周岁的未成年人，请开发者务必确保获得最终用户的父母或其他监护人对于安全监测 SDK 收集、使用最终用户相关个人信息的完整、合法、在使用安全监测 SDK 服务期间持续有效的授权同意。

（3）开发者应向最终用户提供易于操作的访问、更正、删除其个人信息，撤销或更改其授权同意、注销其个人账号实现机制。

2、移动应用安全监测平台支持云服务及私有化两种部署方式，我们希望集成并使用安全监测 SDK 服务的开发者移动应用以合法合规的方式收集、使用最终用户的个人信息。但对于私有化部署方式，我们并不了解且无法控制任何开发者以及他们的移动应用如何使用他们所控制的最终用户个人信息，因此也不应为其行为负责。我们建议最终用户在认真阅读开发者移动应用相关隐私政策，在确认充分了解并同意他们如何收集、使用最终用户的个人信息后再使用开发者移动应用。

3、最终用户具体获得的安全监测 SDK 服务内容由开发者根据其移动应用需要进行选择，可能因为最终用户所使用的开发者移动应用不同而有所差异，安全监测 SDK 可能获得的个人信息取决于最终用户所使用的开发者移动应用的具体类型/版本以及最终用户所使用的功能。如果在部分开发者移动应用版本中不涵盖某些服务内容或未提供特定功能，则本隐私政策中涉及到上述服务/功能及相关个人信息的内容将不适用。

请开发者及最终用户务必认真阅读本隐私政策，在确认充分了解并同意后再集成并使用安全监测 SDK 服务。

本隐私政策将帮助开发者及最终用户了解以下内容:

1. 我们如何收集和使用您的个人信息
2. 我们如何共享、转让、公开披露您的个人信息
3. 我们如何保护您的个人信息
4. 您的个人信息管理权利
5. 您的个人信息如何在全球范围转移
6. 未成年人的个人信息保护
7. 本隐私政策如何更新
8. 如何联系我们

一、我们如何收集和使用您的个人信息

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。我们仅会出于本隐私政策所述的以下目的，收集和使用您的个人信息：

通过采集设备相关信息来用于判断当前 App 所运行的手机设备的安全性，防止恶意的用户对 App 进行网络安全攻击，保护用户的财产安全。

安全监测目前采集的信息主要为系统设备信息，运行过程内存状态信息以及设备位置信息。安全监测产品线，从 2018 年底开始十分重视隐私数据保护，在监测过程中在采集信息过程中遵循 4 个原则：

1、 最小范围原则：只采集对监测、溯源有帮助的信息；

2、 最低敏感度原则：绝不采集个人隐私数据相关的高敏感信息；

3、 不强制原则：不重复申请，不强制授权；

4、 最小影响原则：支持 0 权限启动，保证 90%以上的监测能力不受影响。

目前所涉及的 19 类威胁监测点和 8 类风险监测点（后续仍会增加），其中均已经采取边缘计算技术，以降低对采集信息的依赖程度，具体采集信息的作用详见清单。

Android 信息采集点及用途

信息类别	详细描述	收集方式	用途	采集场景及频次/率
个人位置信息	**GPS 坐标、基站信息**	**通过权限采集**	**1、用于跟踪手机实际位置，判断位置造假； 2、用于实时定位攻击者位置；**	前台操作或前台静默，持续采集
网络身份标识信息	WIFI-MAC, WIFI-SSID,	通过权限采集	1、用于判断是否存在网络信息篡改等风险； 2、用于进行关联分析，找出同一 WIFI、IP 地址的作案团伙；	前台操作或前台静默，仅进行风险检测时采集
	IP 地址	直接采集		前台操作或前台静默，仅进行风险检测时采集
唯一设备识别码	IMEI、IMSI	通过权限采集	1、用于判断是否存在设备伪造等风险； 2、根据客户需要，可能需要和风控系统、银行黑名单对接； 3、作为生成设备指纹的辅助参数；	前台操作或前台静默，仅进行风险检测时采集
	AndroidID	直接采集		前台操作或前台静默，仅进行风险检测时采集

个人常用设备信息	软件列表	直接采集	1、用于风险应用检测； 2、溯源分析阶段，用于辅助判断是否为恶意用户；	前台操作或前台静默，仅进行风险检测时采集
	设备 MAC 地址、硬件序列号	直接采集	1、在客户端作为设备指纹的辅助参数； 2、用于判断是否存在设备信息篡改等风险；	前台操作或前台静默，仅进行风险检测时采集
其他	当前运行应用进程	直接采集	用于风险进程检测	前台操作或前台静默，仅进行风险检测时采集

iOS 信息采集点及用途

信息类别	详细描述	收集方式	用途	
个人位置信息	**GPS 坐标、基站信息**	**通过权限采集**	**1、用于跟踪手机实际位置，判断位置造假； 2、用于实时定位攻击者位置；**	前台操作或前台静默，持续采集
网络身份标识信息	WIFI-SSID、IP 地址	直接采集	1、用于判断是否存在网络信息篡改等风险； 2、用于进行关联分析，找出同一 WIFI、IP 地址的作案团伙；	前台操作或前台静默，仅进行风险检测时采集
个人常用设备信息	软件列表	直接采集	1、风险应用检测； 2、溯源分析阶段，用于辅助判断是否为恶意用户；	前台操作或前台静默，仅进行风险检测时采集
	IDFA、IDFV	直接采集	1、用于判断是否存在设备伪造等风险； 2、根据客户需要，可能需要和风控系统、银行黑名单对接； 3、作为生成设备指纹的辅助参数；	前台操作或前台静默，仅进行风险检测时采集

为了保证您能正常使用集成了移动应用安全监测产品的开发者应用中的安全监测功能及服务，我们会通过开发者应用向您的设备系统申请以下设备权限，申请前我们会征询您的同意，您可以选择“允许”或“禁止”权限申请。经过您的授权后我们会开启相关权限，您可以随时在系统中取消授权，您取消授权会导致您无法使用相关的功能及服务，应用安全监测产品对设备权限的调用情况如下：

Android 设备权限使用

设备权限名称	使用目的	权限授权方式
ACCESS_FINE_LOCATION 访问精准定位	用于跟踪手机实际位置，判断位置造假； 用于实时定位攻击者位置；	授权方式由设备系统开发方以及开发者应用决定； 当您同意向开发者应用授予该

ACCESS_COARSE_LOCATION 访问粗略位置		权限时开启
READ_PHONE_STATE 读取设备信息	用于判断是否存在设备伪造等风险；作为生成设备指纹的辅助参数；	
ACCESS_NETWORK_STATE 识别网络状态	用于判断是否存在网络信息篡改等风险；	
ACCESS_WIFI_STATE 识别 WIFI 状态		

iOS 设备权限使用

设备权限名称	使用目的	权限授权方式
LocationWhenInUseUsageDescription 使用期间访问位置	用于跟踪手机实际位置，判断位置造假；用于实时定位攻击者位置；	授权方式由设备系统开发方以及开发者应用决定； 当您同意向开发者应用授予该权限时开启

位置信息为敏感个人信息，您可以随时通过取消系统授权开发者应用获取相应设备权限或开发者应用提供的其他授权设置停止我们对您的位置信息的收集，之后您可能将无法使用基于位置信息而提供的相关服务或功能，或者无法达到基于位置信息提供的相关服务拟达到的效果。

当我们要将信息用于本隐私政策未载明的其它用途，或者将基于特定目的收集而来的信息用于其他目的时，会事先征求您的同意。但是，在法律允许的范围内，以下情形中，我们可能会未征得您的授权同意而收集或使用您的个人信息：

1、 依据国家法律法规的规定；

2、 依据公检法等执法部门法律程序相关规定；

3、 依据政府部门、上级监管单位的要求；

4、 为维护社会公共利益，保护我们的公司、我们的用户或雇员的合法权益所 合理必需的其他用途。

二、我们如何共享、转让、公开披露您的个人信息

1. 共享

移动应用安全监测平台支持云服务及私有化两种部署方式，对于私有化部署客户，所有信息均在客户私有化环境。我们不会单方与我们的合作方、关联方以外的任何公司、组织和个人分享您的个人信息，

但以下情况除外：

(1) 在获取您明确同意的情况下共享：获得您的明确同意后，我们会与其他方共享您的个人信息。

(2) 我们可能会根据法律法规规定，或按政府主管部门的强制性要求，对外共享您的个人信息。

2. 转让

我们不会将最终用户的个人信息转让给除梆梆安全及其关联方外的任何公司、组织和个人，但以下情形除外：

(1) 事先获得最终用户的明确授权或同意。

(2) 满足法律法规、法律程序的要求或强制性的政府要求或司法裁定。

(3) 如果我们或我们的关联方涉及合并、分立、清算、资产或业务的收购或出售等交易，最终用户的个人信息有可能作为此类交易的一部分而被转移，我们将确保该等信息在转移时的机密性，并要求新的持有最终用户个人信息的公司、组织继续受此隐私政策的约束，否则我们将要求该公司、组织重新向最终用户征求授权同意。

3. 公开披露

我们仅会在以下情形下，公开披露最终用户的个人信息：

(1) 获得最终用户的明确同意；

(2) 基于法律法规、法律程序、诉讼或政府主管部门强制性要求下。

4. 共享、转让、公开披露个人信息时事先征得授权同意的例外

在以下情形中，共享、转让、公开披露最终用户的个人信息无需事先征得最终用户的授权同意：

(1) 与国家安全、国防安全直接相关的；

(2) 与公共安全、公共卫生、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) 出于维护最终用户或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；

(5) 最终用户自行向社会公众公开的个人信息；

(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) 根据个人信息主体要求签订和履行合同所必需的；

(8) 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；

(9) 法律法规规定的其他情形。

根据法律规定，共享、转让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最终用户通知并征得最终用户的同意。

三、我们如何保护您的个人信息

我们已采取了合理、可行的管理措施和技术措施，以保护所处理的个人信息并应对个人信息安全事件。但是请注意，虽然我们采取了合理的措施保护您的个人信息，但没有任何网站、Internet 传输、计算机系统或无线连接是绝对安全的。

具体而言，我们用以保护您提供的个人信息的主要安全防护措施有：

(1) 我们会在可行的情况下及时将您的个人信息进行去标识化处理，从而降低其他组织或个人重新识别到您的风险；

(2) 我们会定期审查个人信息处理的方式（包括物理性安全措施），并不断强化 API 和 SDK 等技术工具的安全性；

(3) 我们将不断努力保障您的个人信息安全，并实施传输全程安全加密等保障手段，以免您的个人信息在未经授权的情况下被访问、使用或披露。

四、您的个人信息管理权利

1. 移动应用安全监测平台提供了云端及私有化部署两种服务方式。所收集的用户个人信息数据均归宿主应用（APP）的开发、运营者所有并由宿主应用（APP）的开发、运营者进行管理。因此，如果您需要查询、更正或者删除本产品收集的与您相关的个人信息，可根据您所适用的国家或地区法律法规，联系 APP 运营者提出行使上述权利的要求。
2. 如果您需要改变您授权同意的范围或撤回您的授权，联系 APP 运营者提出行使上述权利的要求。因为我们产品采集的信息有宿主应用（APP）的开发、运营者进行管理，所以撤回途径、个人信息管理的时效性均以宿主应用的开发、运营者的回复为准。

五、您的个人信息如何在全球范围转移

原则上，我们在中国境内获取和产生的个人信息将存储在中国境内。如部分产品或服务涉及跨境，我们需要向境外传输最终用户的个人信息，我们会严格按照法律法规的规定执行，并保证最终用户的个人信息安全。

若开发者使用我们提供的中国境外服务，则应清楚并理解，不同国家或地区对于数据及个人信息的收集、存储、使用、共享等各有其监管要求，开发者应主动遵守海外国家或地区的法律法规和监管要求。开发者因未遵守相关国家法律法规而引发的相应风险及后果均由开发者自行承担；如我们因此遭受任何形式的诉请、诉求、投诉、处罚等的，开发者将负责全面给予解决；如导致我们或最终用户发生任何形式的损失，开发者负责给予赔偿。同时，我们将保留停止提供相关服务的权利。

在开发者使用我们提供的中国境外服务时，开发者应确保同意或者取得最终用户的同意有关此项跨境传输转移。我们强烈建议开发者咨询当地专业人士，以保证此项跨境传输符合当地的监管要求。特别是，当跨境传输涉及到俄罗斯、印度、欧盟、美国等国家或地区时，请注意这些国家和地区的个人信息监管规定。开发者同意，跨境传输产生的风险和责任将由开发者自行承担；且若最终用户未接受本隐私

政策而由此引发的一切风险及后果亦由开发者自行承担；我们因此遭受任何形式的诉请、诉求、投诉、处罚等的，开发者将负责全面给予解决；如导致我们发生任何形式的损失，开发者负责给予我们全额赔偿。

若开发者在欧盟地区提供服务，我们的业务可能需要我们转移最终用户的个人数据至欧盟以外的国家。这些国家可能提供与欧盟国家不同水平的数据保护。我们作为最终用户个人数据的接收者，会采取适当的措施以确保履行保密义务，并确保如标准合同条款等措施的执行。

六、未成年人个人信息保护

该产品服务可能面向不满 14 岁的未成年人，由于该产品是被宿主应用集成后才为用户提供服务，所以但最终是由集成该产品的宿主应用决定最终用户是否为儿童。如果最终用户是未满 14 周岁的未成年人，请务必在使用已集成开放平台产品及服务的开发者应用前，在父母或其他监护人监护、指导下共同仔细阅读开发者应用隐私政策及本隐私政策，并在征得监护人同意的前提下使用开发者应用或提供个人信息。

我们只会在受到法律允许、父母或监护人同意或者保护未成年人所必要的情况下收集、使用、公开披露未成年的个人信息。如果我们发现在未事先获得可证实的父母同意的情况下收集了未成年人的个人信息，将会采取措施尽快删除相关信息。

七、本隐私政策如何更新

我们的隐私政策可能会不时地更新或适时修改,以适应法律、技术或商业的发展。如该等变更会导致您在本隐私政策项下权利的实质减损，我们将在变更生效前，在页面上提示、发布对本隐私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（对于某些服务，我们会通过电子邮件发送通知，说明隐私政策的具体变更内容）。

本隐私政策所指的重大变更有：

(1) 我们的服务模式发生重大变化：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；

(2) 个人信息共享、转让或公开披露的主要对象发生变化；

(3) 最终用户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；

(4) 其他可能对最终用户的个人信息权益产生重大影响的变化时。

八、如何联系我们

开发者或最终用户对本隐私政策有任何意见、建议、投诉，可拨打客服热线 4008-881-881 或发送邮件至 Service@bangcle.com，工作时间 9-18 点。鉴于最终用户的信息是我们通过开发者的应用收集的，我们建议最终用户优先联系开发者以便得到更高效的反馈。

为保障我们高效处理您的问题并及时向您反馈，需要您提交身份证明、有效联系方式和书面请求及相关证据，我们会在验证您的身份后处理您的请求，并将按照相关法律法规及本隐私政策来维护您的个人信息，并于十五个工作日内予以回复。