华为消费者业务 AI 隐私白皮书

版权所有 © 华为技术有限公司

目 录

1 AI 业务个人信息管理概述 3
1.1 个人信息处理原则 3
1.2 AI 数据生命周期管理 4
2 AI 产品与服务 5
2.1 智慧视觉 5
2.2 智慧语音 6
2.3 智慧识屏 7
2.4 小艺建议 7
2.5 智慧输入法 8
2.6 人脸识别 9
2.7 AI 拍照 9
3 总结 10

版权所有 © 华为技术有限公司

1 AI 业务个人信息管理概述

随着移动互联网发展，云计算服务逐步普及，移动芯片处理能力越来越强大，人工智能算法日趋成熟和完善，以及处理数据爆炸式增加，这些因素驱动了移动领域的 AI 产业高速发展和全面普及。意识到 AI 在移动领域的重要性，华为消费者业务 AI 基于华为 EMUI 系统及 HarmonyOS 进行开发，集成芯片、移动操作系统、云服务，大数据分析的基础能力，集成业界第三方服务提供商在 AI 方面成熟的解决方案能力，提供专注于用户的日常生活和工作场景的 AI 产品和服务，为用户提供更加便利的用户体验。AI 时代机遇与挑战并存，给用户带来更好的产品和服务的同时，也带来了更多的个人隐私安全风险挑战，从用户利益出发，华为始终将合规遵从置于商业利益之上，确保用户的个人信息安全。

1.1 个人信息处理原则

华为对于用户隐私保护以公认隐私保护原则(GAPP)为基础，遵从《中华人民共和国个人信息保护法》、《欧洲通用数据保护条例(GDPR)》和其他各国个人信息保护法律法规。我们对个人信息处理的基本原则如下：

合法、正当、透明：个人信息应当以合法、正当、对数据主体透明的方式被处理。

目的限制：个人信息应当基于具体、明确、合法的目的收集，不应以与此目的不相符的方式作进一步处理。

数据最小化：个人信息应与数据处理目的相关，且是适当、必要的。尽可能对个人信息进行匿名或假名化，降低对数据主体的风险。

准确性：个人信息应当是准确的，并在必要的情况下及时更新。根据数据处理的目的，采取合理的措施确保及时删除或修正不准确的个人信息。

存储期限最小化：存储个人信息不超过实现数据处理目的所必要的期限。

完整性与保密性：根据现有技术能力、实施成本、隐私风险程度和概率采取适度的技术或组织措施确保个人信息的适度安全，包括防止个人信息被意外或非法毁损、丢失、篡改、未授权访问和披露。

可归责：对结果负责并且能够对外展示遵从上述原则。

除了以上基本原则之外，AI 业务中对个人信息收集和处理有额外的要求：本地优先处理原则，个人标识符和传输至云的个人数据分离原则，第三方数据处理受控原则。

1.2 AI 数据生命周期管理

华为提供贯穿整个数据生命周期的隐私安全管理，根据其生命周期各个阶段数据处理活动的特点，提供相应的保护策略。

收集：必须以合法、正当、透明的方式收集与业务目的相关的必要的个人信息。

传输：必须采用安全的方式传输用户的个人信息。

存储：以安全的方式在设备侧或云侧存储用户个人信息，通过技术措施和管理措施对存储数据进行安全防护。

使用：个人信息的使用目的、处理方式和留存期限与向用户展示的隐私通知以及用户的授权范围保持一致。使用过程中提供安全保护机制，防止个人信息泄露或被盗用、误用或滥用。

披露：与第三方协同提供 AI 服务的业务场景下，当华为授权供应商、商业合作伙伴代表华为处理个人信息时，对其进行认证以确保其能够提供安全的个人信息处理措施，并通过合同要求其提供与华为同等的数据保护水平。供应商、商业合作伙伴只能基于与华为的合同、华为指令处理个人信息，不能出于任何其他目的处理个人信息。当华为与独立的第三方共同处理个人信息时，华为会在合同中明确各自的权利义务与应遵循的数据处理规范。

销毁：当用户个人信息留存期限到期时，对数据进行删除或者匿名化，已销毁的数据不能被恢复。

以下以智慧视觉的“识物”功能以及语音助手的“订餐”功能为例展示个人信息收集情况：

识物

数据类型	处理目的	安全防护措施
设备标识	用于灰度升级	HTTPS 安全传输，仅在您开启“智慧视觉改进计划”时才会 AES 加密存储
位置信息	用于基于位置的识别服务，如建筑识别、商店招牌识别等	HTTPS 安全传输,不存储
图片	提取图片中的物体信息用于物体识别、地标建筑识别、商店招牌识别等	HTTPS 安全传输,仅在您开启“智慧视觉改进计划”时才会 AES 加密存储

语音订餐

数据类型	处理目的	安全防护措施
设备标识	用于业务流程中的消息交互	HTTPS 安全传输,AES 加密存储
位置信息	用于查找该位置附近的餐馆美食、当地天气等信息	HTTPS 安全传输,不存储
语音	根据语音指令发送订餐服务请求	HTTPS 安全传输,仅在您开启“智慧语音改进计划”时才会 AES 加密存储

2 AI 产品与服务

华为提供多样化的消费者 AI 产品与服务，为用户的日常生活和工作带来便利，提升用户体验。与此同时，我们非常尊重用户的隐私，我们只会收集和处理 AI 产品或服务所必须的用户数据，数据优先在设备上处理，若需要在华为云上处理，则需要将个人信息经脱敏、加密等措施处理之后经安全传输通道上传至华为云，若个人信息需要发送给第三方处理，则会在用户可知可控的情况下进行，用户可在具体的产品或服务的隐私声明中了解个人信息的详细处理过程。此外，华为充分尊重用户的选择权，用户可自由开启或者关闭各个 AI 产品或服务功能。

2.1 智慧视觉

智慧视觉是华为消费者业务提供的内容识别类应用，通过计算机视觉处理技术对手机摄像头捕捉的图片进行处理，为用户提供物体识别、商品识别、食物卡路里检测、条形码或二维码识别以及文字翻译等服务。

智慧视觉在用户首次使用时会获取用户同意，以收集必要的用户数据提供相应的服务。如果用户不同意或者在后续取消同意，智慧视觉不会收集和处理用户的个人信息。

当用户使用这些服务时，智慧视觉应用集成了业界第三方服务提供商的专业服务能力，与华为的 AI 能力协同一起为用户提供服务。例如，在识物功能中，华为将物体分为宠物、花卉、建筑、名画百图等不同类别，智慧视觉在华为云上对图片中物体进行初步分类之后，需要将图片发给对应的第三方进行识别，由第三方返回识别结果。

为了提供智慧视觉的各类服务，华为需要收集摄像头捕获的图片信息，在商店招牌识别时华为还会获取设备的地理位置信息用于分析商店位置，但华为只将位置信息用于本次服务请求处理，并不保存设备的历史位置记录，也不会分析和跟踪用户的行踪轨迹。由于华为与第三方服务提供商协同一起提供智慧视觉服务，相应的，这些数据也需要发给第三方服务提供商进行处理，但华

为不会将用户的手机号码、华为账号、原始设备标识等发送给第三方，因此第三方不能定位到设备或者个人。此外，诸如第三方购物平台需要进一步将个人信息用于其自身业务目的时，华为会在结果界面上展示第三方服务提供商名称或品牌 Logo。

为了改进智慧视觉产品和提升用户体验，在征得用户同意之后会在手机上开启智慧视觉用户改进体验计划。该功能收集用于识别的图片、随机标识符以及设备相关的其他信息用于改进产品和服务，华为不会使用这些数据对用户进行画像、位置追踪或者推送营销广告。在使用您的图片进行视觉模型训练和改进时，我们会对图片中的敏感信息进行脱敏，如针对人脸使用马赛克遮盖等，以最大程度地保护用户隐私，并且用户可以随时关闭“智慧视觉改进计划”开关以终止该功能。

2.2 智慧语音

智慧语音是华为消费者业务提供的语音识别类应用，通过语音识别、语义识别、自然语言处理等技术对用户语音进行识别、分析和处理，为用户提供语音唤醒、打电话、天气查询、日程查询与设置、打车等服务。

使用智慧语音服务需要用户主动开启语音服务或者使用语音唤醒后使用，并且在首次使用时需要获取用户的同意，如果用户不同意或者后续取消同意，则不能提供智慧语音服务，相应的也不会收集和处理用户的语音数据。

在用户使用智慧语音服务时，华为对敏感个人信息如声纹数据，只会在设备侧进行处理。例如当用户使用语音唤醒功能时，声纹信息经加密保存在手机上，不会上传到华为云或第三方云，用户输入的唤醒语音与声纹仅在设备上进行匹配。又如，用户通过语音进行查询日程时，仅会在手机侧查询日程数据，日程数据不会传输至云。此外，用户还可以使用语音指令接听或挂断电话，这些语音指令也仅仅在手机侧进行处理。

为了更加精确地理解用户的语音指令，智慧语音借助了业界语音处理厂商成熟的语音识别和自然语言处理技术，因此在语音实现模拟点击场景下，如语音订餐、订车、查询天气，华为会将语音数据经加密通道发给第三方语音处理厂商进行语音识别处理，以确认语音指令类型，然后根据音指令类型将相应的服务请求发送给对应的第三方服务提供商。在此过程中，第三方语音处理厂商和服务提供商各司其职，语音识别厂商没有设备标识数据，无法将用户的语音、位置信息与用户的设备相关联，不能对用户进行位置跟踪或者行为分析，而服务提供商不能获取到语音内容，仅根据消息请求接口处理相应的服务请求。

为了改进智慧语音产品和提升用户体验，在用户同意的前提下，智慧语音开启语音助手改进计划功能，该功能收集用户的语音内容、位置信息、匿名化的设备标识符等数据，用于改进产品，提升语音识别准确率。这些数据不会被使用于用户行为分析、位置追踪或者推送营销内容等目的，也不会被披露给第三方，并且用户可以随时关闭该功能。

您可以通过此短片进一步了解智慧语音对个人隐私的保护程度。【附视频短片链接】

2.3 智慧识屏

智慧识屏是华为消费者业务提供的基于手机屏幕的内容识别类应用，用户双指按压屏幕时能对当前屏幕上的内容进行商品识别、文字识别和文本翻译，并生成相应的服务卡片待用户进一步使用。华为不会主动获取用户的屏幕截屏图片或者屏幕上文字信息进行分析处理，只有在用户主动发起双指按压屏幕时才会开启智慧识屏服务，并且在首次使用时需要获得用户同意，如果用户不同意或者后续取消同意，智慧识屏业务不会被开启，相应也不会收集和处理屏幕上的图片或文本信息。

智慧识屏基于图片的商品识别功能会将图片、随机标识符发往第三方购物平台用于识别商品和返回购物链接，协助用户完成一键购物，华为会在结果界面上展示第三方购物平台的名称或者品牌 Logo。

智慧识屏基于文字内容的服务为用户提供分词卡片、服务查询卡片(如电影、音乐、快递单号等)、稍后阅读、全屏翻译等功能。全屏翻译功能由第三方翻译提供商提供，华为只会将待翻译文本发送给第三方，第三方无法将待翻译内容与用户或者设备关联起来。此外，智慧识屏的快递信息跟踪、稍后阅读功能，都只在设备侧处理屏幕上的文本或链接以生成相应的服务卡片，华为以及第三方不会记录用户的快递信息、浏览历史记录等。

类似的，为了提升用户体验，华为提供了智慧识屏改进计划功能。在用户提供单独授权同意的前提下，该功能收集屏幕截图用于优化模型、改进产品，这些数据不会用于用户行为分析或精准广告营销。在使用您的图片进行视觉模型训练和改进时，我们会对图片中的敏感信息进行脱敏，如针对人脸使用马赛克遮盖等，以最大程度地保护用户隐私，并且用户可以随时关闭“智慧识屏改进计划”开关以终止该功能。

2.4 小艺建议

小艺建议是华为消费者业务提供的智能建议类服务，在首次使用时需要用户的主动授权。在用户授权前，小艺建议仅基于用户在本设备上的使用信息进行推荐，且所有的数据处理仅在设备上进行，不会上传到云。在用户授权后，小艺建议会为用户在桌面推荐出用户感兴趣的服务，实现服务的一步直达。

版权所有 © 华为技术有限公司

小艺建议推荐的本地服务，如未接来电、备忘录、日历历程等，这些信息仅会在本地读取和展示，不会上传到云。

为了向您推荐更多丰富的服务，我们提供基于位置的服务推荐，如异常天气等，此时我们仅会向第三方位置服务供应商分享您的粗略位置信息，不会识别到您个人，第三方服务供应商也无法对您进行定位跟踪。

2.5 智慧输入法

智慧输入法是华为开发的输入法应用，除了输入法基本功能外，还能根据用户的基础个人信息(仅在设备侧保存)、聊天上下文等多种信息来源为用户提供精准的候选词，以为用户提供便捷的输入法体验。此外，也提供云输入、语音输入、自动填充（验证码）等智慧化输入功能。

智慧输入法仅在设备上处理用户个人信息。比如智慧输入法的“情感感知”功能，当用户在应用中填写常用的个人信息时，如姓名、邮箱、手机号码、家庭地址等，智慧输入法可以从保存在设备上的基础个人信息数据库获取到这些个人信息作为候选词。当在聊天场景下收到类似询问日程或者行程出行的提问时，智慧输入法会查询设备上的日程信息或出行信息，然后把相应的信息以智能候选词的方式提供。智慧输入法的“智能填充”功能，可以读取手机上短信内容，自动识别并且填充短信验证码，短信内容和验证码都只会在设备上处理。

为了提供用户更准确的候选词，智慧输入法会把用户输入的拼音编码上传至华为云进行查询，返回优化后的候选词，云侧不会保存用户的任何历史输入记录。此外，智慧输入法提供用户上网查询的便捷通道，比如在聊天场景下，当对方询问用户天气、所在地方的美食时，在输入法候选词区域会提供相应的便捷按钮，如“北京天气”、“附近美食”，在用户点击这些按钮时才会触发到第三方业务提供商进行服务查询，查询结果以卡片链接方式展示在输入法界面待用户决定是否发送。

智慧输入法还为用户提供了在线语音输入功能，如果用户选择语音输入，则会将语音经HTTPS 安全传输至第三方进行语音识别，以转换为输入文本。华为不会将设备标识或用户标识传给第三方，因此第三方无法将语音输入与用户或者设备相关联。

2.6 人脸识别

人脸识别，是基于人的脸部特征信息进行身份识别的一种生物识别技术。主要用于人脸解锁及人脸支付场景。

华为终端设备对人脸图像采集、特征提取、特征比对以及特征存储等处理完全在安全隔离的可信环境中进行，HarmonyOS 的人脸框架只负责发起人脸识别和传递识别结果等数据，不涉及人脸数据采集。HarmonyOS 中任何其他第三方应用无法通过 HarmonyOS 人脸识别功能获取到用户人脸数据，也无法将用户人脸数据传出终端设备。

人脸特征数据保存在 TEE 的安全存储中，采用内置安全芯片实现对人脸特征数据的加解密，确保外部无法获取内置安全芯片内的加密密钥，人脸数据不会泄露。

2.7 AI 拍照

华为手机的 AI 拍照功能，通过预置的相机算法，实现特定场景识别（如人像场景、宠物场景、美食、蓝天、沙滩、日落等）和这些场景下的特定处理，比如在人像场景下，实现美肤、虚化和智能构图，用户也可以选择关闭场景识别。

这些 AI 拍照功能仅依赖于预置的相机算法和训练模型，不会收集用户的任何个人信息，也不会上传用户任何个人信息至云上处理或者分享给第三方，所有处理均在设备上完成。

版权所有 © 华为技术有限公司

3 总结

华为高度重视用户的隐私安全，尽可能采用业界最佳隐私保护标准和优秀实践来保护AI 业务场景下的用户个人信息，为用提供安全可信的 AI 服务。

隐私政策声明请参考：https://consumer.huawei.com/cn/legal/privacy-policy

版权所有 © 华为技术有限公司