

AutoPacking 隐私政策

本版更新时间：2022 年【1】月【5】日

【特别提示】本政策适用于我们提供的所有服务。当您使用我们任何单项服务时，您同意接受本政策以及我们在该单项服务中设置的特定隐私信息类政策条款（以下称“特定条款”）的保护，在此情况下特定条款与本政策条款同时对您产生效力。如特定条款与本政策条款存在同类条款的不一致约定，则在特定条款约束范围内应以特定条款为准。如我们提供的某一项服务不适用本政策的，该服务中会以适当方式明示排除适用本政策。

在使用各项服务前，请您务必仔细阅读并透彻理解本政策，特别是以粗体标识的条款，您应重点阅读，在确认充分理解并同意后再开始使用。如果您不同意本政策的内容，将可能导致服务无法正常运行，或者无法达到我们拟达到的服务效果，您应立即停止访问/使用服务。

在阅读完本政策后，如您对本政策或与本政策相关的事宜有任何问题，您可通过[本政策“如何联系我们”](#)章节所列的反馈渠道联系我们，我们会尽快为您作出解答。

本政策将帮助您了解以下内容：

- [一、我们如何收集和使用个人信息](#)
- [二、我们可能共享、转让和披露的个人信息](#)
- [三、我们如何存储和保护个人信息](#)
- [四、修订和通知](#)
- [五、如何联系我们](#)

一、我们如何收集和使用个人信息

我们收集您的个人信息主要是为了您和其他用户能够更容易和更满意地使用服务。

（一）我们将通过以下途径收集和获得您的个人信息：

1、您提供的信息。例如：

（1）您在注册服务的帐号或使用服务时，向我们提供的信息；

请注意，如您在服务中其他用户可见的公开区域内上传或发布的信息中、您对其他用户上传或发布的信息作出的回应中公开您的信息，该等信息可能会被他人收集并加以使用。当您发现他人不正当地收集或使用您的信息时，可通过[本政策“如何联系我们”](#)章节所列的反馈渠道联系我们。

2、我们获取您的信息。您在使用服务时，我们收集、汇总、记录的信息，例如日志信息、位置信息、设备信息。

（二）我们会出于以下目的，收集和使用您以下类型的个人信息：

1、帮助您完成注册及登录

为便于我们为您提供持续稳定的服务并保障您使用服务的安全性，**我们需要您提供基本注册或登录信息，包括手机号码、电子邮箱地址，并创建您的帐号、用户名和密码。**在部分单项服务中，如果您仅需使用浏览、搜索等基本功能，您不需要注册成为用户及提供上述信息。

2、维护基本功能的正常运行

在您使用我们服务过程中，为向您提供浏览、搜索等基本功能，并识别帐号异常状态、了解产品适配性、保障服务的网络及运营安全，以维护前述基本功能的正常运行，**我们可能会直接或者间接地收集、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进行关联，**这些信息包括：

（1）**日志信息**：当您使用我们的服务时（包括后台运行状态），我们可能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：您的登录帐号、搜索查询内容、IP 地址、浏览器的类型、电信运营商、网络环境、使用的语言、访问日期和时间及您访问的网页浏览记录、Push 打开记录、停留时长、刷新记录、发布记录、关注、订阅、收藏及分享。

（2）**设备信息**：当您使用我们的服务时（包括后台运行状态），我们可能会接收并记录您所使用的设备相关信息。例如：设备机型、操作系统及版本、客户端版本、设备分辨率、包名、设备设置、进程及软件列表、设备标识符（MAC 地址/IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息）、软硬件特征信息、设备所在位置相关信息（例如 IP 地址、GPS 位置以及能够提供相关信息的 WLAN 接入点、蓝牙

和基站传感器信息)。为了收集上述基本的个人设备信息,我们将会申请访问您的设备信息的权限,我们收集这些信息是为了向您提供我们基本服务和基础功能,如您拒绝提供上述权限将可能导致您无法使用服务。

请注意,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。如果我们将这类非个人信息与其他信息结合用于识别特定自然人身份,或者将其与个人信息结合使用,则在结合使用期间,这类非个人信息将被视为个人信息,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。这些个人信息在结合使用期间,将作为您的个人信息按照本政策处理与保护。

3、向您提供互动与发布服务

您在使用服务时、上传和/或发布信息以及进行相关互动行为)时,我们将收集您上传、发布的信息,并使用您的昵称、头像和发布内容以作展示。

请注意,您公开发布的信息中可能包含您的个人信息或敏感个人信息,请您在发布前慎重考虑。如您发布的信息涉及到他人的个人信息的,您应当在发布前征得他人同意。

4、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、使用或整合您的帐号信息、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,来综合判断您帐号及交易风险、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。

5、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信息无需征得您的授权同意:

- (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) 与刑事侦查、起诉、审判和判决执行等直接相关的;
- (4) 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;
- (5) 所收集的个人信息是您自行向社会公众公开的;
- (6) 根据您的要求签订和履行合同所必需的;
- (7) 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;
- (8) 开展合法的新闻报道所必需的;
- (9) 法律法规规定的其他情形。

二、我们可能共享、转让或披露的个人信息

(一) 转让

1、随着我们业务的持续发展,我们有可能进行合并、收购、资产转让或类似的交易,而您的信息有可能作为此类交易的一部分而被转移。我们会要求新的持有您个人信息的公司、组织继续受本政策的约束,否则,我们将要求该公司、组织重新向您征求授权同意。

2、在获得您的明确同意后,我们会向第三方转让您的个人信息。

(二) 披露

我们仅会在以下情况下,且采取符合业界标准的安全防护措施的前提下,才会披露您的个人信息:

- 1、根据您的请求,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、法规的要求、强制性的行政执法或司法要求所必须提供您信息的情况下,我们可能会依据所要求的信息类型和披露方式披露您的信息。在符合法律法规的前提下,当我们收到上述披露信息的请求时,我们会要求接收方必须出具与之相应的法律文件,如传票或调查函。我们坚信,对于要求我们提供的信息,应该在法律允许的范围内尽可能保持透明。我们对所有的请求都进行了慎重的审查,以确保其具备合法依据,且仅限于执法部门因特定调查目的且有合法权利获取的数据。

(三) 共享、转让、披露信息时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、与刑事侦查、起诉、审判和判决执行等司法或行政执法直接相关的;

- 4、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；
- 5、您自行向社会公众公开的信息；
- 6、从合法公开披露的信息中收集信息的，如合法的新闻报道、政府信息公开等渠道；
- 7、与我们履行法律法规规定的义务相关的。

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。

三、我们如何存储和保护个人信息

(一) 个人信息的存储

除法律法规或监管部门另有规定外，我们仅在本政策所述目的所必需且最短的时限内存储您的个人信息。如我们终止服务或运营，我们将及时停止继续收集您个人信息的活动，同时会遵守相关法律法规要求提前向您通知，并在终止服务或运营后对您的个人信息进行删除或匿名化处理，但法律法规或监管部门另有规定的除外。

我们在中华人民共和国境内运营中收集和产生的个人信息，存储在中国境内，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、您使用的服务涉及跨境，需要向境外提供您的个人信息。

针对以上情形，我们会确保依据国家法律法规和相关监管部门的规定执行，并对您的个人信息提供足够的保护。

(二) 个人信息的保护

我们非常重视信息安全，成立了专门的安全团队，并采取一切合理可行的措施，保护您的个人信息：

1、数据安全保护措施

我们会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个人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。

我们的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 SSL）对您的个人信息进行加密保存，并通过隔离技术进行隔离，以保护您的个人信息。

在个人信息使用时，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的安全性。

我们还会采用严格的数据访问权限控制和多重身份认证技术保护个人信息，避免数据被违规使用。

2、我们为保护个人信息采取的其他安全措施

我们有行业先进的以数据为核心，围绕数据生命周期进行的数据安全管理体系，从组织建设、制度设计、人员管理、产品技术等方面多维度提升整个系统的安全性。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个人信息的存储和使用。

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。

我们还会举办安全和隐私保护培训课程，加强员工的安全意识以及对于个人信息保护政策和相关规程的认识。

3、我们仅允许有必要知晓这些信息的员工、合作伙伴访问您的个人信息，并为此设置了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个人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的合作关系。

4、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。在通过服务与第三方进行沟通或购买商品及服务时，您不可避免的要向交易对方或潜在的交易对方披露自己的信息，如联络方式或者邮政地址等。请您妥善保护自己的信息，仅在必要的情形下向他人提供。

5、互联网环境并非百分之百安全，我们将尽力确保或担保您发送给我们的个人信息的安全性。如果我们的物理、技术、或管理防护设施遭到破坏，导致个人信息被非授权访问、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。

6、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 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。您需要了解，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。

请您务必妥善保管好您的帐号、密码及其他身份要素。您在使用服务时，我们会通过您的帐号、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。如您发现帐号、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。

四、修订和通知

为了给您提供更好的服务，我们可能会根据服务的更新情况及法律法规的相关要求适时修改本政策的条款，该等修改构成本政策的一部分。我们会在本页面上公布对本政策所作的任何变更。对于重大变更，我们还会提供更为显著的通知（包括网站公告、推送通知、弹窗提示或其他方式），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服务时都查阅我们的隐私政策。

五、如何联系我们

如您有关于网络信息安全的投诉和举报，或您对本政策、的隐私措施、您的信息的相关事宜有任何问题、意见或建议，**请与个人信息保护负责人联系，可发送邮件至 lxz@pku.edu.cn**

一般情况下，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的十五个工作日内予以处理。如您不满意我们的处理，还可以向履行个人信息保护职责的部门进行投诉、举报。