

广州视源电子科技股份有限公司

隐私政策

本隐私政策（以下简称“本政策”）为广州视源电子科技股份有限公司及其关联方（以下简称“视源”“视源股份”或“我们”，）有关个人信息保护的总纲，我们将在本政策中概览性说明视源将如何收集、使用并保护您的个人信息。

我们在向您提供具体的产品和服务时（包括但不限于网站、公众号、小程序、移动应用等），可能会提供单独的隐私政策等文件，具体说明在该产品及服务中的个人信息处理情况，此时，该隐私政策将被优先适用。如具体产品或服务的隐私政策未能涵盖的内容，请您参阅本政策。

本政策将帮助您了解以下内容：

- 一、定义
- 二、我们如何收集和使用个人信息
- 三、我们如何使用 Cookie 和同类技术
- 四、我们如何共享、转移、公开披露您的个人信息
- 五、我们如何保护您的个人信息
- 六、您可以如何行使个人信息相关权利
- 七、个人信息的存储
- 八、未成年人保护
- 九、本政策如何更新
- 十、如何联系我们

一、 定义

“**关联公司**”指因共同所有权或控制权而与视源相关的公司。控制权是指通过所有权、有投票权的股份、合同、实际运营或其他被依法认定的方式直接或间接地拥有影响被控制对象管理/经营的能力。关联公司的范围以视源股份公开发布的最新公告为准。

“**第三方**”指除我们、用户以及我们的关联公司以外的公司、自然人或其他组织机构。

“**个人信息**”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，但不包括匿名化处理后的信息。

“个人信息处理者”是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

“儿童”指不满十四周岁（含）的未成年人。

“去标识化”指通过对个人信息的技术处理，使在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。如采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

“匿名化”指对个人信息进行处理，使之无法识别特定个人且不能复原。

二、 我们如何收集和使用个人信息

我们将根据合法、正当、必要的原则，仅收集实现产品和服务功能所必要的信息用于实现明确、合理的处理目的。

（一）帮助您注册、登录及管理账号

1. 为完成账号创建，您需要提供您的手机号码进行注册，创建用户名和密码。对于支持使用第三方账号授权登录的产品，您也可以使用第三方账号授权我们使用您在第三方账号（例如：微信）注册中提供的信息（例如：微信昵称、头像、性别和地区信息等）。
2. 您可以选择在注册账号后向我们额外提供您的更多个人信息，例如：学校、学科、学段、性别等非注册所必须的个人信息，这将有助于我们向您提供更好的服务和体验。
3. 我们的部分产品和服务使用统一账号体系，对于该等产品，您在使用任一产品时注册账号后无需重复注册即可使用该账号登录统一账号体系下的全部产品。

（二）为您提供具体的产品和服务

1. 在您使用我们某项具体的产品或服务时，例如：课件制作、学校创建、远程会议、购物等，为了向您提供相应的产品或服务，您还需要向我们提供使用该产品或服务所需的信息，例如：课件内容、学校信息、会议信息、收货地址等。
2. 某些产品或服务可能需要您授权我们获取您的设备权限，例如：在您使用上传照片的功能时，我们需要访问您的相册。您可以拒绝授权或关闭设备功能设置停止授权，但这可能导致我们无法向您提供相应的服务或无法达到服务效果。
3. 我们会自动收集您对我们产品的详细使用情况，作为服务日志保存，包括访问日期和时间、浏览记录、点击查看记录、搜索查询记录等，以便我们优化产品和服务。

（三）为了实现安全运行及应用升级服务

我们致力于为您提供安全、可信的产品与使用环境，提供最新、优质而可靠的服务与信息是我们的核心目标。为判断账号安全、进行身份验证、检测及防范安全事件等，我们可能会收集您的 IP 地址、网络接入方式、类型、状态等信息。

（四）客服功能

当您与我们的客服取得联系时，为便于与您联系，记录、解决您提出的相关问题或提升服务质量，我们可能会保存您的沟通、通信/通话记录及相关内容，包括您的联系方式、账号信息、订单信息、收货地址或您为了证明相关事实提供的其他信息。

（五）消息通知

我们还可能会通过您在使用产品或服务的过程中所提供的联系方式（如您的手机号码、邮箱等），向您发送多种类型的通知，例如：消息告知、身份验证、安全验证、用户使用体验调研；此外，我们也可能会以短信、电话的方式，为您提供您可能感兴趣的服务、功能或活动等商业性信息。如您不愿意接受用户使用体验调研与商业性信息，您可以直接与我们联系进行退订。但与消息告知、身份验证、安全验证有关的消息，是为了保障安全与为您提供服务所必需，您无法退订。

（六）接受第三方委托

我们可能会接受您所在组织（例如：您所在的公司、学校以及所属辖区的教育局等）的委托通过我们的产品向您提供服务，此时，您所在的组织为个人信息处理者，我们将按照您所在组织的指示处理您的个人信息。

（七）依法豁免征得同意收集和使用的个人信息

您知晓并同意，根据中华人民共和国法律法规（为本政策之目的，未包括中华人民共和国香港特别行政区法律法规、澳门特别行政区法律法规及台湾地区法律法规，以下简称“法律法规”），在以下情形中，我们收集、使用个人信息无需征得您的授权或同意：

1. 为订立、履行您作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；
2. 为履行法定职责或者法定义务所必需；
3. 为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；
4. 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；
5. 依照相关法律规定在合理的范围内处理您自行公开或者其他已经合法公开的个人信息，对您的个人权益有重大影响或您明确拒绝的除外；

6. 法律、行政法规规定的其他情形。

三、 我们如何使用 Cookie 和同类技术

Cookie 是我们在向您提供服务的过程中向您传输并存储在您设备上的小文件。我们可能会使用 Cookie 或同类技术，如像素标签和网站信标、user agent、local storage。Cookie 可能会在您的设备上存储。为确保产品的正常运转、为您获得更轻松的访问体验，我们通常会利用 Cookie 或/和同类技术，以完成存储和记录您的用户身份数据等功能。大多数浏览器均为用户提供了清除浏览器缓存数据的功能，您可以在浏览器设置中操作清除需要清除的 Cookie 数据，但清除后可能无法使用由我们提供的、依赖于 Cookie 的功能或服务，例如无法记住用户身份，您需要在每次登录时重新填写账号和密码。

四、 我们如何共享、转移、公开披露您的个人信息

（一）共享

我们不会与任何第三方分享您的个人信息，但以下情况除外：

1. 在获取明确同意的情况下共享：获得您的明确同意后，我们会与第三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，与第三方共享您的个人信息。
3. 与我们的关联公司共享：您的个人信息可能会与视源的关联公司共享，共享之前我们会请求取得您的单独同意。我们只会共享必要的个人信息，且受本政策及相关产品或服务隐私政策中所声明目的的约束，例如：部分产品或服务由我们的关联公司提供，为实现使用统一账号登录我们的产品，我们需要在关联公司之间共享您的账号信息。关联公司如要改变个人信息的处理目的、处理方式，将再次征求您的授权同意。
4. 与授权合作伙伴共享：在法律法规允许的范围内，且仅为实现本政策中声明的目的，我们的某些服务将由授权合作伙伴提供。我们可能会与合作伙伴共享您的某些个人信息，以提供更好的客户服务和用户体验，共享之前我们会请求取得您的单独同意。我们仅会出于合法、正当、必要、特定、明确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。我们的合作伙伴无权将共享的个人信息用于任何其他用途。

对我们与之共享个人信息的公司、组织和个人，我们会要求他们遵守我们关于个人信息隐私保护的要求，包括但不限于根据数据保护协议、承诺书以及任何相关的数据处理政策对个人信息进行处理。

（二）转移

我们不会将您的个人信息转移给任何第三方，但以下情况除外：

1. 在获取明确同意的情况下转移：获得您的明确同意后，我们会向其他方转移您的个人信息；
2. 根据适用的法律法规、法律程序的要求、强制性的行政或司法要求所必须的情况下进行转移；
3. 在产品服务提供者因合并、分立、解散或被宣告破产等原因，涉及到需要转移个人信息的，我们会告知您接收方的名称或者姓名和联系方式，并要求新的持有您个人信息的接收方继续受本政策的约束，对于接收方变更原先的处理目的、处理方式的，我们将要求该接收方重新向您征求授权同意。

（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：

1. 获得您的单独同意后；
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。

五、 我们如何保护您的个人信息

我们遵循 ISO 27001 信息安全管理体系及 ISO 27701 隐私信息安全管理体系统，运用各种技术和组织措施及操作规程，对您的个人信息进行保护。此外，我们还会定期测试和评估技术和组织措施的有效性，以确保您的个人信息的安全。

（一）技术保护

为保障您的信息安全，我们努力采取各种符合业界标准的合理的物理、技术和管理方面的安全措施来保护您的信息，使您的信息不会被泄露、毁损或者丢失，包括但不限于网络请求使用 https 加密方式、去标识化、数据中心的访问控制。我们会使用加密技术提高个人信息的安全性；我们会使用受信赖的保护机制防止个人信息遭到恶意攻击；我们会部署访问控制机制，确保只有授权人员才可访问个人信息；我们会对您的个人信息分类管理。

（二）安全体系保证

我们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，我们的信息系统已经获得相应级别的等级保护认证，在组织建设、制度设计、人员管理、产品技术、个人信息安全影响评估等方面多维度保障整个系统的安全性。

（三）人员安全管理

我们明确全体员工在信息安全方面的个人责任，每位员工均有义务维护集团的信息安全。同时，我们对合作的第三方（包括供应商）提出明确的信息安全要求，所有第三方合作方均须遵守信息安全管理有关规定。

我们对可能接触到您的信息的员工或外包人员也采取了严格管理，包括但不限于根据岗位的不同采取不同的权限控制，与他们签署保密协议，监控他们的操作情况等措施。我们会按现有技术提供相应的安全措施来保护您的信息，提供合理的安全保障，我们将尽力做到使您的信息不被泄露、毁损或丢失。我们会举办安全和隐私保护培训课程，制定并组织实施个人信息安全事件应急预案，定期组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程。

（四）信息安全保护提示

1. 请您保管好您登录时所用到的短信验证码及密码，协助我们保证您的账号安全。我们将尽力保障您发送给我们的任何信息的安全性。
2. 您的账号均有安全保护功能，请妥善保管您的账号、短信验证码及密码。我们将通过向其他服务器备份、对用户密码进行加密等安全措施确保您的信息不丢失，不被滥用和变造。但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，我们强烈建议您使用此类工具时请使用复杂密码、定期修改密码、拒绝向他人透露个人账号密码等，并注意保护信息安全。
3. 信息披露提示及验证码泄露处理：我们强烈建议您在使用我们的产品和服务时，务必妥善保管好您的个人信息及其他身份要素。在使用我们的服务时，如果您不可避免地要向交易对方或潜在的交易对方披露自己的个人信息（如联络方式或者邮寄地址），请您仅在必要的情形下向他人提供。如您发现自己的个人信息泄密，尤其是您的账号及短信验证码发生泄露，请您立即联系我们，以便我们采取相应措施。
4. 信息安全事件处理：在不幸发生个人信息安全事件后，我们将按照法律法规的要求向您告知：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。我们将以邮件、信函、电话、推送通知等方式告知您事件相关情况，难以逐一告知个人信息主体时，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，上报个人信息安全事件的处置情况。

5. 互联网环境并非绝对安全，我们将尽力确保您发送给我们的个人信息的安全性。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的绝对安全。您需要了解，您接入我们的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发生问题。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。

（五）信息安全威胁监测与响应机制

我们建立了信息安全威胁监测与响应机制，持续主动监测各类网络安全风险，对安全事件快速响应、及时落地风险缓释措施。若发生数据泄露等安全事件，我们将依法依规处置，向受影响的利益相关方及时告知，充分披露已采取的整改措施及后续防范方案。

六、 您可以如何行使个人信息相关权利

我们尊重您对您个人信息的权利。以下列出您依法享有的权利，以及我们将如何保护您的这些权利，您有权要求我们对个人信息处理规则进行解释说明，具体操作路径请查阅对应产品或服务的隐私政策，您也可以通过本政策“十、如何联系我们”部分所列的联系方式联系我们，以便行使您的权利。请注意，出于安全考虑，在处理您的请求前，我们可能要求验证您的身份。

（一）访问、查询您的个人信息

（二）更正您的个人信息

（三）删除您的个人信息

在以下情形中，您有权向我们提出删除个人信息的请求：

- （1） 如果您决定撤回对我们处理您的个人信息的同意；
- （2） 如果处理目的已实现、无法实现或者为实现处理目的不再必要；
- （3） 如果我们处理个人信息的行为违反法律法规；
- （4） 如果我们收集、使用您的个人信息，却未征得您的同意；
- （5） 如果我们处理个人信息的行为违反了与您的约定；
- （6） 如果您不再使用我们的产品或服务，或您注销了账号；
- （7） 如果我们不再为您提供产品或服务，或者保存期限已届满。

若我们决定响应您的删除请求，我们还将同时通知从我们获得您的个人信息的实体，要求其及时删除，除非法律法规另有规定，或这些实体获得您的独立授权。

当您从我们的产品或服务中删除信息后，我们可能不会立即在备份系统中删除相应的信息，但会在备份系统更新时删除这些信息。如法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，我们会停止除存储和采取必要的安全保护措施之外的处理。

（四）改变您授权同意的范围

您有权限制或者拒绝对您的个人信息进行处理，有权撤回对您个人信息处理的同意，法律法规另有规定的除外。请您理解，每个业务功能需要一些基本的个人信息才能得以完成，当您撤回同意或授权后，我们无法继续为您提供撤回同意或授权所对应的服务，也不再处理您相应的个人信息。但您撤回同意或授权的决定，不会影响此前基于您的授权而开展的个人信息处理。

（五）个人信息主体注销账号

您随时可注销此前注册的账号，我们会在收到您的注销申请并验证您的用户身份后尽快为您处理。在注销账号之后，我们将停止为您提供产品或服务，并在法律法规规定的保存期限届满时删除您的个人信息或做匿名化处理。

（六）个人信息主体获取个人信息副本

您有权获取您的个人信息副本，在技术可行的前提下，例如数据接口匹配，我们还可按您的要求，直接将您的个人信息副本传输给您指定的第三方。

（七）个性化推荐

您有权要求我们进行与您有关的自动化决策。

（八）投诉与举报

我们设置了投诉举报渠道，您的意见将会得到及时的处理。

（九）响应您的上述请求

为保障安全，您可能需要提供书面请求，或以其他方式证明您的身份。我们可能会先要求您验证自己的身份，然后再处理您的请求。

我们将在 15 个工作日内做出答复。对于您合理的请求，我们原则上不收取费用，但对多次重复、超出合理限度的请求，我们将视情况收取一定的成本费用。对于那些无端重复、需要过多技术手段（例如，需要开发新系统或从根本上改变现行惯例）、给他人合法权益带来风险或者非常不切实际的请求，我们可能会予以拒绝。

在以下情形中，我们将无法响应您的请求：

1. 与个人信息处理者履行法律法规规定的义务相关的；
2. 与国家安全、国防安全直接相关的；
3. 与公共安全、公共卫生、重大公共利益直接相关的；
4. 与犯罪侦查、起诉、审判和执行判决等直接相关的；
5. 个人信息处理者有充分证据表明个人信息主体存在主观恶意或滥用权利的；
6. 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同意的，但在紧急情况消除后将及时告知；

7. 响应个人信息主体的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害的；

8. 涉及商业秘密的。

七、 个人信息的存储

（一）存储地点

我们会按照适用的法律法规的要求，将收集的个人信息采取相应的安全加密存储等安全措施存储在中华人民共和国境内服务器上。未经您单独同意，我们不会将您的个人信息传输至境外。

（二）保存期限

除法律法规另有规定外，我们将按如下期限存储您提供的个人信息：

1. 我们会储存您提供的个人信息以满足我们的正当业务需求（例如向您提供服务或者来满足相应的法律、税务以及财务的要求）。

2. 当我们没有这些需要使用到您提供的个人信息的正当业务需求时，或者是法律法规规定的保存期限届满时，或者是您提出删除个人信息的请求或者注销账号时，除非法律法规另有规定外，我们会删除您的个人信息或者对其进行匿名化处理，或者在匿名化或者删除皆不可能实现（例如您的个人信息已经在备份中存储）的时候，安全地储存您的这些个人信息并且将这些个人信息与其他的数据处理区隔开来。

（三）终止运营

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，并在本政策所述目的所必须期间、法律法规及监管要求的保存期限届满后，或终止服务或运营后，对您的个人信息进行删除或匿名化处理，法律法规或监管部门另有规定的除外。

八、 未成年人保护

我们的产品和服务主要是面向十八周岁以上的用户。如果您为未满十八周岁的用户，您应当在使用我们的主要产品和服务之前，征得您的父母或法定监护人的同意。对于我们专门面向儿童的产品和服务，我们会按照法律法规的要求，在征得儿童的父母或监护人的同意下才收集和处理其个人信息，并为产品或服务制定专门的儿童个人信息保护规则。

九、 本政策如何更新

我们的隐私政策可能变更。未经您明确同意，我们不会削减您按照本政策所应享有的权

利。我们会在本页面上发布对本政策所做的任何变更。特定产品和服务的隐私政策有关个人信息处理目的、处理方式和处理的个人信息种类发生变更的，会重新取得您的同意。

十、 决策机构

董事会负责统筹决策信息安全战略、重大信息安全事项，对信息安全相关事项的监督管理承担管理责任。

十一、如何联系我们

我们设立了个人信息保护部门以及任命了相应的个人信息保护专员，如果您对本政策有任何疑问、意见或建议，通过以下方式与我们联系，我们会按照适用法律法规的要求及时向您回复：

个人信息保护专员联系邮箱：compliance@cvte.com

地址：广东省广州市黄埔区云埔四路六号 广州视源电子科技股份有限公司 合规部

我们将尽快审核所涉问题，并在验证您的用户身份后及时予以回复。一般情况下，我们将在 15 个工作日内回复您的请求。如无法响应您的请求，我们会在法律规定的时限要求内，向您发送通知并解释原因。如果您对我们的回复不满意，特别是我们的个人信息处理行为损害了您的合法权益，您还可以向本政策签订地，即广州市黄埔区有管辖权的法院提起诉讼。