

# 保密协议

上海市大数据中心

2024 年【】月

## 使用说明

一、本示范文本主要适用于规范合作方在完成中心非涉及国家秘密项目过程中的保密义务。

二、本示范文本中，“\_\_”空格为需要根据具体情况填写的内容，可针对具体情况进行填写、细化、完善、补充、修改或另行约定；如无填写、细化、完善、补充、修改或另行约定，则填写“无”或划“/”，不可留白。

三、在基于本示范文本起草的合同签约前，应确保所有“\_\_”空格需填写的内容均已填写。在将起草的合同提交给合同相对方前，应删除本示范文本的所有条款说明、风险提示等注释。

# 保密协议

协议编号：\_\_\_\_\_

甲方：上海市大数据中心

联系人：\_\_\_\_\_

联系地址：上海市静安区寿阳路 99 弄 15 号

乙方：\_\_\_\_\_

联系人：\_\_\_\_\_

联系地址：\_\_\_\_\_

鉴于：

在乙方开展\_\_\_\_\_项目（以下简称**项目**）的过程中，包括本协议生效前、生效后、甲乙双方磋商阶段以及履行与项目有关的协议期间，乙方将获悉相关保密信息（范围见本协议第一条定义）。

为了明确乙方就保密信息所应承担的保密义务，双方本着平等自愿、公平诚信的原则，依据《中华人民共和国民法典》《中华人民共和国保守国家秘密法》《中华人民共和国反不正当竞争法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》及相关法律法规订立本协议。

## 第一条 定义

1.1. 本协议所称保密信息包括：

- (1) 《中华人民共和国保守国家秘密法》及相关法律法规规定的国家秘密；
- (2) 项目涉及的任何商业秘密、保密商务信息、个人信息和隐私；
- (3) 甲方向乙方提供的（包括但不限于直接、间接、口头、书面、电子文件或其他任

何方式提供), 或者乙方以任何方式获得的, 以及虽属于第三方但甲方承担保密义务的项目相关数据、资料、信息等无论是否记载或标注“注意保密”或“绝密”“机密”“秘密”“内部”等字样的信息;

(4) 乙方因开展项目工作的原因进入甲方指定工作场所而接触到的信息和项目涉及的服务器或终端计算机或软件运行中获取的任何个人信息及数据、组织数据、行为数据等数据以及因项目产生的任何商业、营销、技术、运营数据和其他性质的资料等虽未被标注“注意保密”或者“绝密”“机密”“秘密”“内部”等字样, 但从其内容、性质等判断, 具有保密属性的信息, 包括但不限于源代码、计算机程序、数据表、网络关系列表、网络拓扑结构、技术参数和信息、技术秘密、财务信息、商业秘密、保密商务信息、会议纪要、在幻灯片放映以及其他演讲过程中披露的信息、人员名册和个人信息、调查、报告、解释、预测、设计构思和规划、发展研讨、说明书、设计图、图表、范例、设备资料、价格资料、客户和供应商资料和信息、内部决策等;

(5) 以任何方式反映出来的有关甲方及其主管单位、所属分支机构不宜向第三方透露或向社会公众公开的信息和资料;

(6) 甲方作为该项目建设单位, 受该项目牵头单位\_\_\_\_\_委托进行建设, 并交付该项目使用单位\_\_\_\_\_使用(以下简称**项目牵头单位和使用单位**); 项目牵头单位和使用单位向乙方提供(包括但不限于口头、书面、电子文件或任何其他方式)的任何标注“注意保密”或“绝密”“机密”“秘密”“内部”等字样的信息;

(7) 甲方及其主管单位、该项目牵头单位和使用单位未批准公开的事项, 如工作场所情况、单位运行机制、内部规章制度和有关政策与程序、发展规划、会议纪要等;

(8) 为完成项目签订或形成的任何合同、协议、承诺书、会议纪要、备忘录等;

(9) 乙方通过调研等方式获取的项目相关数据、资料、信息等;

(10) 为完成项目相关工作形成的任何研究成果、结论性意见、项目报告等成果性信息;

(11) 甲方、该项目牵头单位和使用单位明示或默示要求乙方应予以保密的其他信息;

(12) 其他\_\_\_\_\_。

1.2. 特别地, 双方在此确认, 在任何情况下, 项目涉及的服务器、计算机、计算机系统或信息系统内的所有系统配置、技术参数和业务数据、信息以及计算机系统或应用系统的漏洞信息虽不能标注“注意保密”或“绝密”“机密”“秘密”“内部”等字样, 但同样属于保密信息。甲方和项目牵头单位和使用单位的机构设置、运行机制、业务流程、逻辑流程, 甲方和项目牵头单位和使用单位的服务器、计算机、信息系统或应用系统的功能、交易量、交易特征、配置、参数、业务数据, 和甲方、项目牵头单位和使用单位与其他组织(包括本协议中的乙方)的合作信息、合同, 以及基于所有合作交流、委托协议、技术合同、合作协议所形成或开发出来的成果(包括但不限于程序运行、程序维护所取得或形成的任何数据、资料、中间成果等), 均属于甲方和项目牵头单位和使用单位的保密信息, 甲方和项目牵头单位和使用单位间的关于保密信息的权属、管理责任等依照上海市有关规定确定。任何国家秘密、商业秘密、保密商务信息以及个人信息和隐私(无论是否在前文有所表述), 在任何情况下, 均属于保密信息。

1.3. 本条 1.1 款和 1.2 款的所有信息合称为“保密信息”。

## **第二条 保密义务**

对第一条所称的保密信息, 乙方同意并保证承担以下保密义务:

2.1. 乙方应对保密信息采取严格的保密措施并履行相应的保密义务, 该等保密措施以及保密义务的严格程度应当符合国家法律法规要求和保密相关规定, 并且不低于乙方对属于自身拥有的相同或相似属性保密信息所采取的保密措施的严格程度。乙方应当具有相应的保密资质(如涉及), 具备完善的保密制度, 以及符合国家保密规定和标准的场所、设施、设备等条件, 并派遣专门的人员负责保密工作。

2.2. 上述第 2.1. 款所指的保密措施以及相关的保密义务包括以下内容:

(1) 除本协议第 2.3. 款约定的情况外, 未经甲方事先书面同意, 乙方不得向任何第三方单位、个人或公众以任何形式告知、披露、公开或提供全部或者部分保密信息或者允许第三方使用保密信息。

(2) 乙方仅可为项目或者与项目有关协议的目的而使用第一条所述保密信息, 不得将保密信息用于任何其他目的, 不得私自窃取、复制、留存保密信息。

(3) 涉及《中华人民共和国保守国家秘密法》及相关行政法规、规章规定的国家秘密事项, 不得向境外组织或个人披露。因项目工作需要向境外组织或个人提供的, 应当按照《中华人民共和国保守国家秘密法》等规定办理。本协议约定的除国家秘密之外的保密信息, 乙方向其现在与未来境内或境外的总公司、分公司、母公司、子公司、办事处及其他关联企业、营业组织或与本约有关的员工、顾问、代理人、合作伙伴(合称为“乙方相关方”, 以下出现的**乙方相关方**, 均与此定义相同)披露或授权其使用保密信息时, 应确保该等披露、授权仅能在为了项目和与项目有关协议的框架内以及必要的范围内进行, 并且在进行该等披露或者授权之前, 乙方应先经过甲方书面同意且与该乙方相关方签订保密协议, 以要求该乙方相关方按不低于本协议的规定要求对保密信息保密。与乙方相关方签订的保密协议应当约定以下事项: (a) 如乙方相关方为自然人的, 则该等自然人不得将保密信息向其他方披露或者授权其他方使用, 而仅能在保密协议约定范围内(在任何情况下不得超出本协议约定的范围)使用该保密信息; (b) 如乙方相关方为单位的, 则在该保密协议中应当明确可以获得并使用该保密信息的自然人的明细, 且获得该等保密信息的自然人不得将上述保密信息再向其他方披露或者授权其他方使用, 而仅能在其与乙方相关方之间的保密协议范围内(在任何情况下不得超出本协议约定的范围)使用。

在本协议项下, 乙方必须和全体涉及项目的乙方相关方签订保密协议, 乙方与乙方相关方所签订的前述保密协议应当向甲方提供备份。乙方应当制定保密方案, 就参与此项目的人员可接触保密信息的范围、账户使用权限等事项进行明确, 并报甲方书面同意。就参与此项

目的人员，乙方应在该等人员接触保密信息以前对其进行保密审查并进行保密教育，就乙方派驻甲方和该项目牵头单位和使用单位参与项目的人员（含新增或变更人员）应在入驻指定工作场所前至少一周以书面形式通知甲方。乙方应当确保其与本项目相关的工作人员因调动工作、退休等原因调离甲方指定工作场所甚至离开乙方单位的，应及时交还使用、借用的所有与项目相关的资料及其他储存介质，并与该工作人员进行保密谈话，要求其继续履行保密义务，并就谈话内容作书面记录。乙方对乙方相关方及乙方相关方的员工、顾问、代理、合作伙伴等违反保密义务给甲方造成的全部损失承担连带赔偿责任。

此外，向境外组织或者个人提供数据的，应当符合《中华人民共和国数据安全法》及相关法律法规的要求。

（4）如出现保密信息丢失、被盗、被泄露或使用，乙方应当尽一切合理努力采取有效措施防止泄密进一步扩大，并在得知保密信息泄露后立即向甲方书面报告，并积极配合甲方和司法机关进行调查。

（5）乙方在服务过程中应遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等法律法规、政策规定的要求，严格按照“同步规划、同步建设、同步使用”原则落实项目安全技术措施，将系统安全运营相关监控措施纳入方案。

（6）若项目为涉密项目，乙方应接受甲方保密延伸检查。

（7）在服务过程中，乙方应在甲方限定的办公区域内、访问或使用甲方限定的信息资产（包括但不限于场地办公设施、计算机、服务器等），并在规定的-safe环境中进行数据处理、开发测试、运维监控等活动，遵守环境安全监控的要求，在开发测试工作中，不得使用真实数据、不得越级操作。

（8）提供服务过程中，若涉及开源软件、组件等产品的使用，乙方应在使用前向甲方提供项目涉及产品的完整清单，并附相应产品的漏洞扫描报告、安全评估报告等证明材料，

审核通过后方可使用。

(9) 乙方提供服务过程中须保障现有系统的网络通畅、系统可用和数据安全。严格落实网络和数据安全防护能力、密码应用、信创应用等运维、运营工作要求，配合开展系统等级保护定级、密码应用安全性评估等工作。

(10) 乙方在提供服务过程中，被甲方或第三方测评机构检测出安全漏洞、等保/密评测评未通过，乙方须在规定时限内完成整改并提供复测报告，逾期未整改到位的，甲方有权按照约定追究乙方违约责任。

(11) 乙方须提供自身的网络与数据安全管理制度、保密管理制度，并在中标后提供人员、财务及安全管理情况报告，发生造成甲方及项目受影响的变动，应及时向甲方报告；

(12) 乙方应对乙方人员开展安全培训，并与其签订保密协议，且保证用于项目实施工作的相关终端安装正版杀毒软件及防火墙。

(13) 提供服务过程中，乙方需要对收集到的所有信息严格管理，严禁在网络上传播、散布和出售，牟取商业利益；乙方人员不得以任何方式泄露、公开或传播项目涉及的内容及成果；不得非法篡改数据、非法入侵甲方网络，不得影响数据的完整性及可用性；不得留存任何安全风险隐患；参与项目建设与质保、维修的个人，不得私自拷贝和留存上述信息副本。

(14) 乙方指定专人负责项目实施过程中的安全工作，接受甲方数据安全部门的直接管理和考核，协助开展安全检查等工作。

(15) 乙方若需互联网端功能测试，应经甲方批准同意，结束后应及时关闭测试系统，删除测试数据，并将结果及时报备甲方。

(16) 乙方通过项目获取的甲方数据禁止超过合同限定范围使用，以及违规转发第三方；

(17) 乙方应按甲方规定申请数据服务接口，加强认证和鉴权防护，保护甲方数据不被泄露。

(18) 乙方禁止将管理后台、数据库服务端口暴露在互联网。



(19) 乙方应加强对乙方人员的安全管理。进入项目前，乙方人员应参加安全培训并通过考核，接受背景调查，提供本人无犯罪记录证明，与甲方签订保密协议。入场前，乙方人员应填写入场申请，按需申请系统账号、云桌面账号和工位。入场后，乙方人员应在甲方规定的安全环境中进行数据处理、开发测试、运维监控等活动，遵守环境安全监控的要求，禁止共用账号、拍照等。在开发测试工作中，依据要求将数据脱敏使用，禁止将数据导入个人电脑、将甲方代码或数据泄露或公开。禁止个人私自搭服务端和共享网络、终端跨互联网和政务外网。禁止在互联网传输甲方文件。非驻场人员，按需提出入网申请，并安装终端管理工具。禁止将甲方数据在个人电脑上留存使用，因需求调研或设计获取数据的，禁止将甲方数据外发，或存储在共有云上，数据使用后应进行销毁。

2.3. 如果国家司法、行政、监察、立法等机关依法要求乙方披露任何保密信息，乙方应当立刻（在收到有关机关通知后 1 小时口头，4 小时内书面）将此事通知甲方并协助甲方处理相关事项。经甲方书面同意，乙方可以将被依法要求必须披露的信息披露给提出披露要求的机关，但披露内容仅限于相应机关要求披露的信息，乙方应做出合理程度的努力使披露的保密信息得到可靠的保密待遇。

2.4. 如果获得保密信息的乙方相关方存在任何在本协议项下会被认定为违约的行为，无论该乙方相关方是否构成其与乙方之间根据上述第二条第 2.2 款第 (3) 项所签订的保密协议项下的违约，乙方均应当采取一切合理手段（包括但不限于司法程序）来制止该乙方相关方在未经授权的情况下披露或使用保密信息，并根据本协议第七条的约定向甲方承担违约责任。

### **第三条 保密义务的例外**

3.1. 乙方对下述信息不承担保密义务：

(1) 乙方在获悉此保密信息前已经拥有或未利用甲方、该项目牵头单位和使用单位任何条件的情况下独自开发的信息且对此无保密义务（但甲方、该项目牵头单位和使用单位表

示乙方必须就该等保密信息予以保密的除外);

(2) 乙方从合法持有并有权合法披露的第三方获取的信息且对该信息无保密义务;

(3) 在甲方、该项目牵头单位和使用单位披露信息之前已经被公众所知的, 同时有书面记录佐证该公开性质, 且乙方获得该等信息并未违反本协议或者其他保密责任或义务;

(4) 由甲方、该项目牵头单位和使用单位自行或与其他第三方合作(共同)公开或者披露的信息;

(5) 经甲方、该项目牵头单位和使用单位书面许可批准对外公布或公开使用的信息。

在任何情况下, 上述保密义务的例外并不排除乙方根据法律法规规定对国家秘密、商业秘密、保密商务信息、个人信息和隐私等所承担的法定义务和责任。

#### **第四条 保密信息的返还及销毁**

4.1. 在项目开展过程中、项目完成、与项目有关的协议终止或者无论因任何原因解除后, 乙方及乙方相关方均应当按照甲方要求立即将所有其获得的或者持有的保密信息(包括但不限于图画、说明书、照片、设计、计划书以及其他文件)及其储存于任何介质中任何形式的副本、复制件、翻译件等归还甲方, 或者根据甲方的要求以不可恢复方式予以销毁或删除, 并确保乙方及乙方相关方不再持有保密信息, 包括但不限于保密信息的复制品、翻译件等。如果甲方要求乙方及乙方相关方销毁包含保密信息的材料, 乙方及乙方相关方应同时确保保密信息从服务器或计算机或其他电子系统中删除或抹掉, 同时乙方及乙方相关方应向甲方出具销毁证明文件并加盖公章, 销毁证明文件中应具体说明哪些书面资料、硬件或电子文档等载体已被销毁。

#### **第五条 甲方的监督权利**

5.1. 在项目实施过程中, 甲方享有以下权利:

(1) 甲方有在合理范围内监督、限制乙方活动(包括但不限于使用涉及保密信息的活动和分包活动)的权利, 有权对乙方执行本协议的情况进行监督检查, 对不符合约定的事项,

乙方应及时纠正并向甲方提交书面整改报告；

(2) 经事先书面告知乙方，甲方有权对乙方使用设备终端、软件实施必要、适当且合理的管制措施；

(3) 经事先书面告知乙方，甲方有权聘用第三方专业机构对项目的实施过程进行监督但甲方的监督行为会违反相关法律法规的除外。

## **第六条 保密期限**

6.1. 在本协议项下，乙方就保密信息所承担的保密义务自获悉保密信息之日起持续有效，且无论本协议或者项目和/或与项目有关的协议以何种事由终止或者解除，该等保密义务持续有效，乙方应当继续履行保密义务。

## **第七条 违约责任**

7.1. 如果乙方未履行本协议所规定的保密义务，甲方有权根据法律法规规定或本协议约定追究乙方违约责任，包括但不限于：

(1) 要求乙方立即实际履行保密义务，并停止相关违约行为；

(2) 终止双方的合作业务（无论双方合作业务协议中是否有特殊说明）；

(3) 要求乙方按照：a) 甲方的相关管理规定；b) 乙方因违约所得的收益；或 c) 甲方因此所遭受的损失【包括但不限于直接损失、间接损失（例如因保密信息被公开而损失的该保密信息可实现的预期利益价值、甲方因调查及处理侵害行为所支出的所有费用等）、损害赔偿金（例如甲方因乙方泄露保密信息而被第三方追责要求支付的赔偿金）、律师费、诉讼费/仲裁费、公证费、调查费、保全担保/保险费等】，向甲方进行赔偿，甲方有权选择上述 a)、b)、c) 中的任何一种方式向乙方主张违约责任，如甲乙双方无法就上述 a) 或 b) 或 c) 的内容达成一致的，则乙方应按照项目中标金额（如项目经过招投标程序）或项目总价款（如项目未经招投标程序）的 30% 向甲方支付违约金；

(4) 如乙方违约对甲方声誉等造成其他影响的，甲方有权采取其他一切措施维护自身

权益。

甲方有权选择上述约定中的一个或多个追究乙方责任。

7.2. 如乙方相关方存在任何在本协议项下视为违约的行为，则视为乙方构成违约，甲方有权按照本协议第七条约定追究乙方的违约责任。

7.3. 在任何情况下，本协议第七条并不排除甲方或者任何其他方在法律法规项下就违反保密义务的行为向相关方追究其他民事、行政、刑事责任的权利。

### **第八条 非特许或授权**

8.1. 本协议并非授予或暗示任何专利、著作权、商标、商业秘密或其他知识产权项下的许可或权利。

### **第九条 法律适用与争议解决**

9.1. 本协议适用中华人民共和国法律。任何因执行本协议而发生的纠纷，可以由双方协商解决，协商不成的，任何一方都可以向甲方所在地有管辖权的人民法院提起诉讼。

### **第十条 完整协议**

10.1. 本协议构成双方之间关于项目保密义务和责任的协议，如双方之间就项目所签订的相关协议或者合同中就同样事宜具有其他约定，则相关的义务和责任要求应当按照最严格的原则一并适用。

10.2. 如本协议某一个或多个条款全部或部分无效或无法执行，剩余的条款或任何部分可执行的条款应当仍具有约束力，双方应当共同遵守。

### **第十一条 其他**

11.1. 本协议自双方加盖公章之日起生效。本协议一式贰份，甲乙双方各执壹份，具有同等效力。对本协议的任何修改须采用书面形式，经双方加盖公章方为有效。本协议条款亦适用于双方各自的权利和义务的继受人。

**【以下无正文】**

【本页为\_\_\_\_\_项目《保密协议》签字页，无正文】

甲方：上海市大数据中心

日期：\_\_\_\_年\_\_月\_\_日

乙方：\_\_\_\_\_

日期：\_\_\_\_年\_\_月\_\_日