附件

温州市公共数据授权运营申报指引

|  |  |  |  |
| --- | --- | --- | --- |
| 资料清单 | | | |
| 序号 | 材料名称 | 文件要求 | 备注 |
|  | 公共数据授权运营申请表 | 原件加盖公章 | 1份 |
|  | 授权运营应用场景说明 | 原件加盖公章 | 1份 |
|  | 统一社会信用代码证件 | 复印件加盖公章 | 1份 |
|  | 法定代表人身份证明 | 原件加盖公章 | 1份 |
|  | 经办人授权委托书 | 原件加盖公章 | 1份 |
|  | 经办人身份证明 | 原件加盖公章 | 1份 |
|  | 近一年第三方审计报告 | 复印件加盖公章 | 1份 |
|  | 近一年第三方财务会计报告 | 复印件加盖公章 | 1份 |
|  | 数据安全承诺书 | 原件加盖公章 | 1份 |
|  | 安全风险自评报告 | 原件加盖公章 | 1份 |
|  | 具有符合网络安全等级保护三级标准和商用密码安全性评估要求的系统开发和运维实践经验 | 复印件加盖公章 | 1份 |
|  | 企业信用报告 | 复印件加盖公章 | 1份 |
|  | 无重大违法记录说明 | 原件加盖公章 | 1份 |
|  | 一般纳税人证明 | 复印件加盖公章 | 1份 |
|  | 其他佐证材料 |  |  |
| 注:  1.提交材料涉及签字、盖章部分，需由签字人签字、加盖单位盖章。无法亲笔签署的，需提交授权人委托他人签字的授权委托书，授权委托书应为原件，且授权人应亲笔签字，被委托人应配合温州市数据局进行实名认证。  2.请将所有材料以PDF格式单独命名并标序，打包发送至指定邮箱：wzdao@wenzhou.gov.cn；压缩包命名格式：“授权运营申请-单位名称-场景名称”。 | | | |

# 材料1

## 公共数据授权运营申请表

|  |  |  |  |
| --- | --- | --- | --- |
| 授权运营单位 |  | 统一社会信用  代码 |  |
| 法定代表人 |  | 安全负责人 |  |
| 单位联系人 |  | 联系电话 |  |
| 通讯地址 |  | | |
| 企业性质 | □国有独资 □国有控股 □集体企业  □私营企业 □股份制 □其他 | | |
| 企业简介  （限300字） | （内容包括但不限于企业相关资质能力、从事的行业、是否设立数据安全管理部门、企业从事数据服务业务年限、专业人员数量（如：技术/法务等）、员工总人数等内容） | | |
| 场景名称 |  | | |
| 行业领域 |  | 数据产品和服务形态 | （如API、数据报告等形式） |
| 应用场景描述 | 描述数据产品和服务涵盖的应用场景。 | | |
| 数据产品和服务内容与标准 | 描述数据产品和服务的内容和标准，包括：  1.服务对象；  2.服务用户数；  3.并发。 | | |
| 预期成效 | 描述数据产品和服务的经济效益、社会效益等。 | | |
| 应用绩效评估 | 1.提供哪些服务（为解决该领域哪些问题提供数据支撑）；  2.回流数据清单；  3.其他可量化的应用绩效评估指标。 | | |
| 单位意见：  本公司将遵守相关法律法规、行业自律等各项规定，本申请表填报的各项内容均真实、完整、合法、有效，自愿维护温州市公共数据授权运营秩序，遵循公共数据授权运营相关规则，接受相关行业部门指导与监督。    单位（公章）：  法定代表人或经办人签字：  年 月 日 | | | |

# 材料2

## 授权运营应用场景说明

（应用场景名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_）

一、用户需求分析

（一）问题分析

问题导向，分析当前场景下所存在的堵点和痛点问题，说明什么人群、在什么场景下，存在什么样的问题。如存在多个问题需逐一说明。

（二）用户需求分析

按场景分析各类问题所对应的用户需求，说明什么人群在什么场景需要什么服务。

（三）行业分析

分析相关行业的现状与前景，分析其优势和不足，发现未被满足的用户需求和市场机遇。

二、应用场景描述

（一）应用场景

基于需求分析，系统阐述作品提供哪些核心能力，每一能力包括服务于哪些人群，各解决什么问题。

（二）功能描述

基于用户需求，系统阐述作品的核心功能点，以及每一个功能点具体的作用。

（三）可实施性

应用场景具有较强的可实施性，明确授权运营期限内的目标和计划。

三、数据加工说明

结合应用场景和原型展示，说明背后的数据加工实现方式。例如：如何对数据进行加工和融合，使用的算法模型，出入参等等。

四、社会经济效益分析

说明产品所产生的社会效益和经济效益（包含商业模式），从定性、定量两个维度说明产生的预期成效。

五、应急预案

## 附：数据申请清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | IRS系统数据表/接口名称 | 数据表英文名称/接口编码 | 数源单位 | 数据项名称 | 数据项英文名称 | 数据使用说明 |
|  |  |  |  |  |  |  |
|  |  |
|  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# 材料3

## 统一社会信用代码证件

具有有效合法营业执照、税务登记证、组织机构代码证或三证合一营业执照。

# 材料4

## 法定代表人身份证明

姓名： 性别： 年龄： 职务：

系 （法人名称）的法定代表人。

特此证明。

附：法定代表人身份证复印件(需同时提供正面及背面)

单位名称： （盖单位章）

日期： 年 月 日

# 材料5

## 经办人授权委托书

本人 （身份证件号码： ）系 （公司名称）的法定代表人，现授权我单位 （身份证件号码： ）为公共数据授权运营申请工作经办人。经办人代表我单位进行申请工作过程中的一切行为，包括所签署和上传的资料，我单位均予以承认，并将承担相应的法律责任。

授权委托期限： 年 月 日至 年 月 日

单位名称（盖章）：

法定代表人（签字）：

经 办 人（签字）：

日期： 年 月 日

# 材料6

## 经办人身份证明

姓名： 性别： 年龄： 职务：

系 （单位名称）的合法正式员工。

特此证明。

附：经办人身份证复印件(需同时提供正面及背面)

单位名称（盖单位章）：

日期： 年 月 日

# 材料7

## 近一年第三方审计报告

# 材料8

## 近一年第三方财务会计报告

# 材料9

## 数据安全承诺书

温州市数据局:

为保障公共数据安全，依法保护个人信息，本单位在获取利用公共数据过程中，郑重承诺遵守本承诺书的有关条款，切实做好数据安全和个人信息保护工作并承担相应法律责任。

一、本单位承诺遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《浙江省公共数据条例》《浙江省公共数据授权运营管理办法（试行）》《温州市公共数据授权运营管理办法（试行）》及有关法律、法规、规章的规定。

二、本单位承诺健全数据安全管理制度，对本单位公共数据授权运营相关的岗位人员、系统平台、技术应用、对外合作等实施全面的安全管理。

三、涉及个人信息、商业秘密、保密商务信息的公共数据，应经过脱敏、脱密处理，或经相关数据所指向的特定自然人、法人和非法人组织依法授权同意后获取。

四、本单位承诺如发现数据安全隐患或其它不安全因素，应第一时间上报公共数据主管部门，并密切配合做好数据安全事件的处置及调查工作，采取措施消除安全隐患。

五、近３年未发生网络安全或数据安全事件。本单位承诺一旦发现有关数据已经泄露或可能泄露，立即通知公共数据主管部门，共同采取相应措施，查找相关工作人员和泄漏原因、线索和证据，并承担相应责任。

六、若违反本承诺书有关条款和国家相关法律法规的，本单位直接承担相应法律责任，侵犯商业秘密、个人隐私等他人合法权益或造成财产损失的，由本单位直接赔偿并且销毁有关数据。同时，贵单位有权暂停或停止运营授权。

七、本承诺书自签署之日起生效并遵行。

单位名称（盖章）：

法定代表人或经办人（签字）：

日期： 年 月 日

# 材料10

公共数据授权运营

安全风险自评报告

（供参考）

填报单位（盖章）：

填报时间： 年 月 日

说明：

1.授权运营申请单位需针对《安全风险自查表》中每项评估要点进行自评，并提供相应证明或说明材料作为本安全风险自评报告的附件一同提交，无法提供相应证明或说明材料，也无法进行相应承诺的，请在备注栏说明理由。

2.授权运营申请单位承诺提供的所有材料准确、真实、合法、有效，并愿为此承担有关法律责任。

安全风险自评报告

一、自评概述

（一）评估目的（请勾选）

□1.摸清授权运营全流程数据处理活动的情况；

□2.若涉及自有数据或社会数据融合，摸清数据种类、规模、分布等基本情况，对数据的来源、归属和流转进行阐述，并提供在授权运营实施过程中详细的数据图谱或目录；

□3.发现可能影响国家安全、公共利益或者个人、组织合法权益的数据安全问题和风险；

□4.发现对外提供、交易、委托处理、向境外提供数据等处理活动的数据安全问题和风险；

□5.促进完善数据安全保护措施，提升数据安全保护能力。

□6.其他：

（二）评估结论概要

说明数据安全风险评估结果概要。

二、授权运营相关情况

（一）授权运营单位基本情况

说明数据处理者的机构实体基本情况。基本情况包括但不限于：

1.单位名称、组织机构代码、办公地址、法定代表人信息、所属行业领域、数据安全负责人及其职务、联系方式、申请单位网络安全/数据安全相关资质、认证情况，以及安全人员的规模、安全相关资质、参与授权运营场景数据处理人员名单等基本信息；

2.是否具有符合网络安全等级保护三级标准和商用密码安全性评估要求的系统开发和运维实践经验（需附证明材料）；

3.近3年是否发生过网络安全、数据安全事件或个人信息保护相关安全事件，以及攻击威胁情况；

4.资本组成、股权结构和实际控制人情况；

5.是否存在违约、违规和失信记录。

（二）授权运营场景情况

1.场景业务基本信息，包括业务描述、业务类型、服务对象、业务流程、用户规模、覆盖地域等基本信息。若授权运营场景须通过开发App、信息系统、小程序等形式提供数据产品或服务的，应说明涉及防火墙、入侵检测、入侵防御等网络安全设备、安全人员及策略情况，设备、系统及用户的账号口令管理情况。

2.场景业务涉及个人信息、重要数据、核心数据、商业秘密、保密商务信息的，应当详细列出处理的数据种类，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

3.外部导入数据情况（若存在自有数据或社会数据导入情形的，需评估以下情况）：

外部导入数据清单（含字段名、类别、级别等）、数据范围、行业领域、数据规模、敏感程度、数据来源合法性与合规性、数据形态、与场景的关联性、数据处理方式方法等。

4.授权数据是否再转移、对外提供；

5.授权数据是否向境外提供（若为“是”，需评估以下内容）：

（1）是否属于不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形；

（2）因业务需要确需向境外提供的，预计一年内向境外提供1万人以上、不满100万人个人信息的：（请勾选）

□基于个人同意向境外提供个人信息；

□与境外接收方订立个人信息出境标准合同并向省级网信部门备案；

□通过个人信息保护认证；

□申报数据出境安全评估。

因业务需要确需向境外提供的，预计一年内向境外提供100万人以上个人信息的，是否申报数据出境安全评估（需附证明材料）。

6.是否存在第三方参与的数据加工活动。

三、安全措施情况

（一）数据安全管理制度情况。

1.网络安全和数据安全责任制度；

2.人员管理和访问权限制度；

3.数据分级分类管理制度；

4.数据安全风险感知响应机制，并承诺在开展公共数据运营过程中，因数据汇聚、关联分析等原因发现数据间隐含关系与规律，并危害国家安全、公共利益，或侵犯个人信息、商业秘密、保密商务信息的，立即停止相应的数据处理活动，并及时向公共数据主管部门报告数据风险情况；

5.应急预案及处置机制；

6.安全日志审计制度；

7.安全事件追踪溯源制度；

8.安全教育培训制度；

9.第三方监督管理机制；

10.投诉、举报、调查、问责制度；

11.安全问责制度等。

（二）安全技术保障能力

身份鉴别和认证、数据收集采集安全管理、数据分类分级、数据存储备份、加密传输、国家商用密码算法、数据脱敏、去标识化、加密技术、数据防泄漏、数据接口安全管理、数据销毁处置、安全漏洞发现与修复、网络日志审查及留存、泄露数据溯源排查、安全风险事件应急处置及补救措施等能力。

三、风险分析与评价

分析安全风险，进行风险评价。具体风险分析和评价方法，可参考《信息安全技术 数据安全风险评估方法（征求意见稿）》。

（一）风险分析

1.数据安全管理风险识别

2.数据处理活动风险识别

3.数据安全技术风险识别

4.个人信息处理风险识别

（二）风险评价（可选）

综合风险危害程度及风险发生可能性对安全风险进行综合评价，自评结果：存在重大安全风险、高安全风险、中安全风险、低安全风险、轻微安全风险。

（三）自评整改

针对发现的数据安全问题或风险，提出整改措施或风险处置措施。措施包括不限于以下选项：

1.预处理阶段对某些类型数据进行销毁；

2.缩小处理范围；

3.采取额外的技术措施；

4.加强对应数据处理活动岗位人员培训；

5.匿名化、去标识化；

6.完善管理制度；

7.采用其他数据处理技术；

8.修订隐私条款；

9.完善与第三方的协议（如有）；

10.其他措施。

附：

安全风险自查表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 一、是否建立并实际落实了完善的数据安全管理制度，包括但不限于： | | | | |
| 序号 | 评估要点 | 自评结果 | 主要参照 | 备注 |
|  | 网络安全和数据安全责任制，明确数据安全责任人； | □有 □无 | 《中华人民共和国网络安全法》第21条、第25条以及相关规定  《中华人民共和国数据安全法》第27条、第29条至第32条以及相关规定  《中华人民共和国个人信息保护法》第51条至第59条以及相关规定  《浙江省数字经济促进条例》第19条至第22条以及相关规定  《浙江省公共数据条例》第33条以及相关规定  《浙江省公共数据开放与安全管理暂行办法》第30条以及相关规定  《信息安全技术 数据安全能力成熟度模型（GBT 37988-2019）》相关规定  《信息安全技术 个人信息安全规范（GBT 35273-2020）》相关规定  《网络安全标准实践指南 网络数据安全风险评估实施指引TC260-PG-20231A》相关规定  《浙江省公共数据安全体系建设指南（DB33/T 2487-2022）》相关规定  《浙江省公共数据授权运营管理办法（试行）》相关规定  网络安全部门和征信部门的监管数据 |  |
|  | 人员管理和访问权限制度； | □有 □无 |  |
|  | 数据分级分类管理制度； | □有 □无 |  |
|  | 数据安全风险感知响应机制； | □有 □无 |  |
|  | 应急预案及处置机制； | □有 □无 |  |
|  | 安全日志审计制度； | □有 □无 |  |
|  | 安全事件追踪溯源制度； | □有 □无 |  |
|  | 安全教育培训制度； | □有 □无 |  |
|  | 第三方监督管理机制； | □有 □无 |  |
|  | 投诉、举报、调查、问责制度； | □有 □无 |  |
|  | 安全问责制度； | □有 □无 |  |
|  | 近3年是否发生过网络安全、数据安全或个人信息保护相关的安全事件； | □是 □否 |  |
|  | 是否有安全事件应对处置及评估的记录，并按规定向主管部门报告。 | □是 □否 |  |
| 二、是否具备足够的安全技术保障能力，包括但不限于： | | | | |
| 序号 | 评估要点 | 自评结果 | 主要参照 | 备注 |
|  | 具备身份鉴别和认证能力； | □是 □否 | 《中华人民共和国网络安全法》第21条、第25条、第42条以及相关规定  《中华人民共和国数据安全法》第27条、第29条至第32条以及相关规定  《中华人民共和国个人信息保护法》第20条至第25条、第51条至第59条以及相关规定  《网络数据安全管理条例（征求意见稿）》〔1〕相关规定  《浙江省公共数据条例》第33条以及相关规定  《浙江省公共数据开放与安全管理暂行办法》第30条以及相关规定  《信息安全技术 网络安全等级保护基本要求（GB/T 22239-2019）》相关规定  《信息安全技术 数据安全能力成熟度模型（GB/T 37988-2019）》相关规定  《信息安全技术 个人信息安全规范（GB/T 35273-2020）》相关规定  《信息安全技术 个人信息安全规范（GB/T 35273-2020）》相关规定  《信息安全技术 信息系统密码应用基本要求（GB/T39786-2021）》相关规定  《信息安全技术 网络数据处理安全要求（GB\_T 41479-2022）》相关规定  《网络安全标准实践指南 网络数据安全风险评估实施指引TC260-PG-20231A》相关规定  《浙江省公共数据安全体系建设指南（DB33/T 2487-2022）》相关规定  《浙江省公共数据授权运营管理办法（试行）》相关规定 |  |
|  | 具备数据收集采集安全管理能力； | □是 □否 |  |
|  | 具备数据分类分级能力； | □是 □否 |  |
|  | 具备数据存储备份能力； | □是 □否 |  |
|  | 具备加密传输能力； | □是 □否 |  |
|  | 具备国家商用密码算法； | □是 □否 |  |
|  | 具备网络可用性管理能力； | □是 □否 |  |
|  | 具备数据脱敏、去标识化、加密技术能力； | □是 □否 |  |
|  | 具备数据防泄漏能力； | □是 □否 |  |
|  | 具备数据接口安全管理能力； | □是 □否 |  |
|  | 具备数据销毁处置能力； | □是 □否 |  |
|  | 具备安全漏洞发现与修复能力； | □是 □否 |  |
|  | 具备防范计算机病毒和网络攻击、网络入侵能力； | □是 □否 |  |
|  | 具备网络日志审查及留存能力； | □是 □否 |  |
|  | 具备安全风险事件应急处置及补救措施等能力； | □是 □否 |  |
|  | 是否存在第三方参与的数据加工活动？（若为“否”无需评估第30-34项） | □是 □否 |  |
|  | 确保第三方的数据安全保障能力是否与授权运营单位一致； | □是 □否 |  |
|  | 不存在授权数据向未经授权的第三方泄露的可能性； | □是 □否 |  |
|  | 采取审计、背景调查、尽职调查等方式审核及监督参与数据加工活动的第三方的数据安全保障能力及数据处理活动； | □是 □否 |  |
|  | 与第三方在合作协议中约定网络、数据安全相关的约束条款，包括终端安全、网络安全、数据安全、保密管理等要求； | □有 □无 |  |
|  | 监督第三方是否擅自留存、使用、泄露或向他人提供授权数据。 | □是 □否 |  |
| 三、用于接收、存储、传输和处理授权数据的终端、系统、应用等，是否包括但不限于确保满足如下要求： | | | | |
| 序号 | 评估要点 | 自评结果 | 主要参照 | 备注 |
|  | 安全物理环境； | □有 □无 | 《信息安全技术 网络安全等级保护定级指南（GA/T 1389-2017）》相关规定  《信息安全技术 网络安全等级保护基本要求（GB/T 22239-2019）》相关规定  《信息安全技术 网络安全等级保护实施指南（GB/T 25058-2019）》相关规定  《信息安全技术 信息系统密码应用基本要求 GB/T39786-2021》相关规定  《浙江省公共数据授权运营管理办法（试行）》相关规定 |  |
|  | 安全通信网络； | □有 □无 |  |
|  | 安全区域边界； | □有 □无 |  |
|  | 安全计算环境； | □有 □无 |  |
|  | 安全管理中心； | □有 □无 |  |
|  | 安全建设管理； | □有 □无 |  |
|  | 安全运维管理。 | □有 □无 |  |
| 四、是否存在对数据再转移、对外提供的情况？（若为“否”无需评估第42项） | | | | □是 □否 |
| 序号 | 评估要点 | 自评结果 | 主要参照 | 备注 |
|  | 若是，是否对数据接收方进行安全监督？ | □是 □否 | 《网络数据安全管理条例（征求意见稿）》相关规定 |  |
| 五、是否存在授权数据出境的可能性？（若为“否”无需评估第43-45项） | | | | □是 □否 |
| 序号 | 评估要点 | 自评结果 | 主要参照 | 备注 |
|  | 因业务需要确需向境外提供的，是否开展数据出境安全自评估或个人信息保护影响评估； | □是 □否 | 《中华人民共和国网络安全法》第37条  《中华人民共和国数据安全法》相关规定  《中华人民共和国个人信息保护法》第38条至第43条、第55条、第56条以及相关规定  《数据出境安全评估办法》第3条、第5条  《规范和促进数据跨境流动规定（征求意见稿）》〔2〕相关规定  《网络安全审查办法》相关规定  《数据出境安全评估办法》相关规定  《个人信息出境安全评估办法（征求意见稿）》〔3〕相关规定  《浙江省数据出境自评估索引指南（第一版）》相关规定 |  |
|  | 因业务需要确需向境外提供的，是否属于不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情况。 | □是 □否 |  |
|  | 因业务需要确需向境外提供的，是否按照相关法律法规及有关要求进行出境安全评估审核。 | □是 □否 |  |
| 六、拟申请的受限开放类数据，经过脱敏、去标识化处理后是否存在被还原的可能性。 | | | | |
| 序号 | 评估要点 | 自评结果 | 主要参照 | 备注 |
|  | 是否可以通过分离、高维数据、关联数据、推断等方法被重标识； | □是 □否 | 《信息安全技术 个人信息去标识化指南（GB/T 37964-2019）》相关规定  《信息安全技术 数据安全能力成熟度模型（GB/T 37988-2019）》相关规定  《网络数据安全管理条例（征求意见稿）》相关规定  《浙江省公共数据授权运营管理办法（试行）》相关规定 |  |
|  | 是否监控去标识化效果； | □是 □否 |  |
|  | 是否提供面向不同数据类型的脱敏方案,可基于场景需求自定义脱敏规则； | □是 □否 |  |
|  | 是否对数据脱敏处理过程相应的操作进行记录，以满足数据脱敏处理安全审计要求。 | □是 □否 |  |
| 七、是否对重要数据和敏感个人信息进行重点保护。 | | | | □是 □否 |
| 序号 | 评估要点 | 自评结果 | 主要参照 | 备注 |
|  | 对重要数据、个人信息的关键操作（例如批量修改、拷贝、删除、下载等）,设置内部审批和审计流程,并严格执行; | □有 □无 | 《信息安全技术 个人信息安全规范（GB/T 35273-2020）》相关规定  《信息安全技术 网络数据处理安全要求（GB\_T 41479-2022）》相关规定  《信息安全技术 重要数据处理安全要求（征求意见稿）》〔4〕相关规定 |  |
|  | 及时对个人信息做删除或匿名化处理; | □有 □无 |  |
|  | 传输重要数据和敏感个人信息时,采用加密、脱敏等安全措施。 | □有 □无 |  |
| 八、是否存在违约、违规和失信记录。 | | | | □是 □否 |
| 九、根据公共数据主管部门或上级部门要求，确需评估的其他内容。（可另附并在自评报告中说明） | | | | |
| 填报人： 联系方式： | | | | |

注：

〔1〕《网络数据安全管理条例》尚未正式出台，目前引用自国家互联网信息办公室官网在2021年11月14日公布的征求意见稿文本，后续正式出台后以正式文本为准。

〔2〕《规范和促进数据跨境流动规定》尚未正式出台，目前引用自国家互联网信息办公室官网在2023年9月28日公布的征求意见稿文稿，后续正式出台后以正式本文为准。

〔3〕《个人信息出境安全评估办法》尚未正式出台，目前引用自国家互联网信息办公室官网在2019年6月13日公布的征求意见稿文本，后续正式出台后以正式文本为准。

〔4〕《信息安全技术 重要数据处理安全要求》尚未正式出台，目前引用自全国标准信息公共服务平台公布的征求意见稿文本（2023年8月10日），后续正式出台后以正式文本为准。

# 材料11

## 具备相关开发和运维实践经验

提供具有符合网络安全等级保护三级标准和商用密码安全性评估要求的系统开发和运维实践经验的佐证材料。

包含但不限于：相关开发或运维合同、相关系统三级等保证明、相关系统密评证明、相关系统截图等。

# 材料12

## 企业信用报告

登陆[国家企业信用信息公示系统(https://www.gsxt.gov.cn)](https://www.gsxt.gov.cn/index.html)，输入企业名称点击查询，在查询结果界面提供如下系统查询结果截图：

1.基本信息查询结果

2.行政处罚信息查询结果

3.列入经营异常名录信息查询结果

4.列入严重违法失信名单（黑名单）信息查询结果

# 材料13

## 无重大违法记录说明

温州市数据局：

我司及法定代表人近三年内无任何重大违法记录。

我司及法定代表人未被列入失信被执行人名单、重大税收违法案件当事人名单、严重失信名单。

特此声明。

单位名称（盖章）：

法定代表人（签字）:

日期： 年 月 日

# 材料14

## 一般纳税人证明

提供税务机关官网一般纳税人资格查询结果截图或税务机关出具的有效证明材料或近半年开具过的增值税发票。