

员工隐私权声明

FIS 处理员工（临时工、正式工、合同工、独立承包商、学生、退休人员以及曾在 FIS 担任此类职务的人员）的个人数据，以及与公司员工有关的其他人员的个人数据。

FIS 员工个人数据的主要控制者是雇用、签约或聘用员工的 FIS 公司。如果你对收集信息的公司有任何疑问，请通过人事支持中心提交工单。

员工个人数据包括在与 FIS 的工作关系中收集和处理的个人数据。FIS 还处理与员工、合同工、独立承包商、学生、退休人员和曾在 FIS 担任此类职务的人员有关系的亲属、受抚养人和其他人（如果其个人数据已被与 FIS 有工作关系的人员提供给 FIS）的个人数据。

在某些司法管辖区，根据适用法律被视为“敏感个人数据”的员工个人数据可能需要根据当地法律的要求或允许（例如，为遵守平等机会法案或当地税收要求）进行收集。敏感个人数据的定义因国家/地区而异。你可在此浏览不同类别的敏感个人数据。请注意，这并不意味着 FIS 将为每个员工处理所有列出的潜在敏感个人数据；只有在适用法律要求或允许的情况下，或在 FIS 为追求合法利益而认为必要且始终遵守适用法律的情况下，才会进行处理。在某些情况下，适用的当地法律可能要求数据主体同意处理敏感个人数据。

门禁卡信息

FIS 的所有员工都将获得门禁卡，以便进入我们的设施。在某些司法管辖区，在适用法律授权的情况下，我们将监控门禁卡的使用记录，以用于安全、工作场所管理和员工出勤管理目的。这包括与管理人分享个人门禁卡使用和团队的门禁卡使用数据，以提供进入指定办公室/设施的团队成员数量的总体视图。

可处理的员工个人数据类别如下：

| 数据类别 | 示例 |
|------------|------------------------------------|
| 申请人数据 | 简历、求职信、申请表、面试时提供的信息、成功申请人入职时提供的信息。 |
| 建议、意见和其他评论 | 员工满意度调查、离职面谈。 |

员工隐私声明

| 数据类别 | 示例 |
|-------------------|--|
| 考勤数据 | 缺勤、休假申请、考勤记录、带薪和无薪休假记录。 |
| 银行及财务资料 | 工资和/或费用报销直接存款银行信息，信用卡信息。 |
| 福利数据 | 员工和/或其受抚养人（如果参加了福利延续计划）参加的福利计划记录、保险、授权书等文件。 |
| 商务差旅和出差数据 | 旅行数据，包括旅行日程、住宿、交通工具、膳食和其他费用。 |
| 公司财产发放数据 | 公司发放的资产、设备和车辆的记录。 |
| 薪酬数据 | 基本工资、奖金和其他薪酬要素、薪酬类型、薪酬等级、薪酬水平、全职当量（FTE）、货币、薪酬请求（过去和现在）、雇佣条款、养老金计划编号和缴费、非薪酬福利、股票期权。 |
| 受抚养人信息 | 受抚养人和重要他人的个人联系方式和身份数据，包括出生日期和性别。 |
| 纪律处分数据 | 警告、训诫信、书面和口头警告。 |
| 就业相关数据 | 员工编号、签名、就业状态、社保号、税号、保险号码、居住国、国籍、照片、紧急联系人、护照信息、移民身份、旅行签证信息、工作和居留许可。 |
| 投诉数据 | 投诉、仲裁数据。 |
| 记录在公司系统、设备或文件中的信息 | 电子邮件、短信、网站使用情况、语音邮件记录、日历或日记条目、通信，包括员工或独立承包商在公司系统、设备或文件中包含的员工个人数据、背景和信用调查数据。 |
| 工作信息和工作指标 | 职位、职称、劳动合同、工资单 ID、直属经理、职位等级、绩效记录、就业状态、工作时间记录、培训记录、绩效目标和发展目标。在某些情况下，FIS 也可能记录能力评估结果、安全报告和事件、专业反馈。 |
| 门禁卡和门禁记录 | 进入和离开受控设施的日期、时间和地点，计算机和系统登录/注销审计跟踪。 |
| 兵役状况 | 服役军种、军衔、入伍或退伍日期、退伍状态、伤残退伍军人身份、获得的奖项或勋章、受保护的退伍军人身份。 |
| 组织内部数据 | 名称、公司结构、组织构架图、汇报关系、职务、简历、工作联系方式、电子邮件、会计科目明细表、雇佣条款、职位描述和薪资水平。 |

员工隐私声明

| 数据类别 | 示例 |
|--------------|--|
| 父母/监护人数据 | 16 岁以下学生的父母/监护人的姓名、签名和同意。 |
| 工资处理数据 | 姓名、政府颁发的身份证、家庭住址、电子邮件、考勤记录、报酬、薪酬数据、入职日期、离职日期、雇佣条款、受抚养人数据、银行和财务数据、福利数据、会计科目明细表、预扣税款和扣款，以及员工出资的福利登记信息。 |
| 绩效和雇佣 | 绩效评估、绩效改进计划 (PIP)、绩效辅导、纪律处分、感谢信、绩效投诉的详细信息。 |
| 个人详细信息和联系方式 | 姓名、性别、出生日期、出生地点和国家、家庭住址、电话号码、电子邮件、政府颁发的身份证号码、公司颁发的或代表公司颁发的识别号码、签名、笔迹和照片。 |
| 照片、视频或音频记录 | 安全系统、闭路电视、个人照片、带照片的安全徽章、语音邮件、培训录制、会议或营销材料收集的信息。 |
| 招聘和申请数据 | 申请详情、申请人测试、背景调查、招聘人员编写的与申请人有关的说明以及筛选结果。 |
| 不当行为或违反政策的举报 | 与员工涉嫌或已确认的不当行为或违反公司政策有关的类似举报记录，无论举报是通过口头、书面、电子邮件、电话，还是通过公司道德热线网站、公司道德热线、内部威胁情报响应团队 (InTIRT)、金融服务信息风险团队 (FSIRT)、安全事件响应倡议和政策 (SIRI-P)。 |
| 工作权/移民数据 | 工作权证明文件、国籍、居留权、公民身份、护照和签证信息。 |
| 软件应用程序 | 使用软件应用程序处理员工数据（包括与参与和协作相关的数据），以提高 FIS 的效率。 |
| 人才、教育和培训详情 | 教育、技能、工作经验、以前的工作、成就、项目、发展和培训、语言技能、技术技能、教育背景、专业认证和注册、专业机构和组织成员资格。 |
| 工作经历 | 聘用和/或解聘日期、职称、晋升日期、参加过的培训课程、对公司政策的签署、完成公司各种强制性培训的情况及测验分数（如适用）、离职或解聘原因、担任的公职、发表过的出版物。 |
| 工作时间表数据 | 计划和实际工作时间、计费 and 行政时间记录、雇佣条款、替代工作安排（远程）。 |

员工隐私声明

| 数据类别 | 示例 |
|----------|-------------|
| 工作场所安全数据 | 报告、照片、视频记录。 |

以下是一些可能被处理的**员工敏感个人数据**的潜在类型列表：

| 敏感个人数据类别 | 示例 |
|---------------------------|---|
| 生物特征和健康数据 | 指纹、拇指指纹、疫苗接种状态、体温扫描、面部识别和声纹。 |
| 揭示犯罪、刑事定罪的数据，或从安全措施中获得的信息 | 刑事诉讼、结果和判决、驾驶记录、先前工作经历、药物滥用筛查、法庭记录和背景调查信息。 |
| 揭示性生活的数据 | 受抚养人和重要他人的个人联系方式和身份数据、婚姻/伴侣关系状态、住宿和住房信息。 |
| 揭示个人信用和财务信息的数据 | 信用调查、子女抚养、债务偿还、破产、查封、工资扣除、银行账号。 |
| 揭示身体或精神健康或状况的数据 | 身体限制和特殊需求、残疾和所需的合理便利、现场检查、公司转介医疗或咨询支持、药物滥用检测、医疗报告、健康证明。 |
| 揭示种族或民族出身的数据 | 种族名称、国籍和文化认同。 |
| 揭示宗教信仰或类似性质的其他信仰的数据 | 与宗教组织的隶属关系、宗教团体的成员资格（例如，出于税务目的而要求）、宗教偏好或其他信仰的声明。 |
| 揭示工会成员资格的数据 | 工会或工会协议会记录、目录、会议文件和其他材料。 |
| 揭示政治观点的数据 | 专业和其他隶属关系、担任的职务、发表过的出版物和著作。 |
| 个人身份信息 | 护照信息、社保号或州身份证号码。 |

FIS 处理员工个人数据的目的：

- 人力资源管理，包括组织和个人管理，工时管理，改进和保持有效的员工管理，内部员工分析，报告和规划；
- 薪酬和福利计划，包含员工及其受抚养人的工资、奖金、养老金、医疗福利、保险政策、休假和请假；

员工隐私声明

- 多元化计划，包括遵守多元化目标、FIS 管控的表彰和奖励计划、与就业相关的教育、培训和认知计划；
- 全球流动计划和员工及其受抚养人的调动、搬迁和流动；
- 人力、人员配备和继任计划；
- 工资、薪酬和福利管理，包括提供员工福利、维持薪资、薪酬、知识产权、津贴、福利、保险、养老金和绩效评估；
- 工资、税款和其他规定的预扣款项（如法院命令的扣款）、差旅费报销和其他可报销的业务费用；
- 人才管理和获取，包括招聘、评估适合性和工作能力、背景调查、资格验证、获取和提供推荐信；
- 学习与发展管理，包括认证、员工培训、执行评估和员工满意度调查；
- 与入职和离职相关的流程，包括内部调动和解聘；
- 病假、其他请假和休假管理；
- 工作场所和员工健康；
- 内部健康和计划，包括健康、安全和事故记录，或报告和管理流程质量；
- 差旅和费用管理以及出差管理，包括对出差人员数据进行监测，以便在安全或医疗紧急情况下提供支持；提供差旅安全、健康和培训，并在自愿的基础上协助在紧急情况下提供安全支持；
- 业务运营，包括人员配置建议、客户计费、业务过渡活动、业务谈判和交易；
- 履行就业和社会保障法或集体协议规定的义务并行使特定权利；
- FIS 组织的内部和外部沟通；
- FIS 的代表，包括商业登记和授权委托书；
- 组织 FIS 活动（包括管理和组织内部非营销相关活动、项目和会议），并对这些活动进行记录；
- 意见和员工满意度调查；
- 管理 FIS 资产，包括员工或其他人的照片和视频，这些照片和视频可在 FIS 的内网、网站等地方下载；
- 财务和共享会计服务，提供记录到报告、订单到现金和采购到付款服务；
- 重组、收购和出售业务、业务单元和公司；
- 业务报告、统计和分析；
- 监督和审计员工在工作场所的活动是否符合 FIS 的公司规定、政策、合同义务和法律要求，包括纪律处分；
- 开展审计、审查和监管检查，以履行对监管机构的义务；
- 对工作场所涉嫌违反政策、与工作、安全和保障问题有关的不当行为进行调查；
- 诉讼或潜在诉讼；

员工隐私声明

- 公司治理、风险管理和合规性，包括遵守法律、执法机构、法院和监管机构的要求，以及预防、侦查、调查和补救犯罪、欺诈或违禁活动，或以其他方式维护法律权利并建立、行使或维护法律主张；
- 管理供应商、承包商、顾问和其他专业专家，包括联系互动、处理和履行采购和发票，以及合同生命周期管理；
- 利用工作绩效和产品，并参考图纸、采购订单、销售订单、发票、报告等文件；
- 工作场所和员工安全保障，例如指纹、面部识别等，用于计算机、电话、建筑物和门禁的设备和安全访问。
- 门禁系统，为授权人员进入和/或离开有出入限制的地点提供电子控制，并在紧急情况下对现场人员进行登记；
- 入侵检测，包括第三方对紧急情况、周边、内部安全点和辅助监控系统（用于现场维护/自动化系统）的监控；
- 维护和保护产品、设施、服务、系统、网络、计算机和信息的安全，预防和侦查安全威胁、欺诈或其他犯罪或恶意活动，并确认业务连续性；
- 管理 IT 资源，包括基础设施管理（包括数据备份）、信息系统支持和应用程序管理服务运营、终端用户支持、测试、维护、安全（事故响应、风险、漏洞、违规响应）、主数据和工作场所（包括用户账户管理、软件许可证分配、安全和性能测试以及业务连续性）。

从员工处收集的某些个人数据涉及其近亲和紧急联系人。在这种情况下，FIS 将要求员工告知相关人员其个人数据将如何根据本声明进行处理。

如果公司员工在第三方的场所工作（例如在客户地点或场所），则该第三方可能需要出于其自己的目的以数据控制者的身份处理该员工的个人数据。在这种情况下，公司员工将收到或可以要求相关数据控制者发出单独的隐私声明。

接收方

出于合法的业务需求和/或流程，员工个人数据可能会被披露给以下接收方或接收方类别：FIS 人力资源管理、法务部、公司合规部、风险管理部、并购团队、安全部、供应链管理和房地产部、内部审计部、财务和会计部、信息系统部、董事会成员、管理人员、FIS 客户和 FIS 选择的服务提供商。FIS 还可能会根据授权向其他第三方提供员工个人数据，例如执法机构、税务机关、其他公共机构、FIS 公司或业务的潜在和实际收购者（如果预期或发生所有权变更或业务转让）。有关 FIS 向哪些类别的实体披露这些信息以及披露信息的目的的更多信息，请参阅“FIS 与谁共享你的个人数据”。

员工隐私声明

存储限制和其他相关信息

员工个人数据将被保留至不再有业务需求或法律法规要求为止。有关 FIS 数据保留标准的更多信息，请参阅公司内网 [FIS&me](#) 上“FIS 企业政策办公室”中的《记录管理政策》。如果你是求职者、退休人员或其他无法进入 FIS 内部系统查看此类政策的人员，请直接向 FIS [隐私办公室](#) 索取此类信息。

行使你的权利

请点击[此处](#)，了解你作为数据主体根据适用隐私和数据保护法所享有的权利概览，以及如何行使这些权利。

FIS 处理员工及其相关人员个人数据的法律依据是：

| | |
|---|---|
| <p>为了履行 FIS 与员工签订的任何劳动合同或其他雇佣合同以及相关集体协议的义务，或者作为建立雇佣关系或其他合同关系的合同前措施的一部分。</p> | <p>GDPR 第 6.1.b 条 中国个人信息保护法 第 13.(2) 条</p> |
| <p>在某些情况下，且仅在所在国家/地区法律允许的情况下，FIS 会根据公司合法利益来处理员工个人数据，前提是这不会凌驾于个人的隐私利益之上。这些合法利益可能包括：</p> <ul style="list-style-type: none">○ 发展和管理 FIS 的员工队伍；○ 分析绩效并提供适当的薪酬○ 平等机会监测和报告；○ 保留商业记录，确保设施和系统安全，并将联系方式提供给相关同事和客户；○ 推广、提供产品和服务，开拓业务机会；○ 维护设施、系统和 IT 基础设施的安全和完整性；○ 监控（例如通过 IT 系统）、调查和确认遵守法律、法规、标准以及 FIS 内部的要求和政策；○ 预防欺诈和犯罪活动，包括调查此类活动，防止滥用 FIS 资产、产品和服务，并在必要和适当的情况下确认网络和信息安全；○ 进行制裁和反洗钱筛查并履行监管要求； | <p>GDPR 第 6.1.f 条 中国个人信息保护法第 13.(2) 条</p> |

员工隐私声明

| | |
|--|---|
| <ul style="list-style-type: none"> ○ 出于必要的内部管理目的（例如提供集中服务），在 FIS 集团内部传输个人数据； ○ 促进和改善健康、安全、保障和绩效 <p>(* 例如，在中国，根据《个人信息保护法》（PIPL），合法利益不被视为处理个人数据的法律依据。在中国，FIS 根据与员工签订的劳动合同（或其他聘用合同）并按照中国法律制定的内部雇佣规则，处理上述目的处理员工个人数据。</p> | |
| <p>在某些情况下，FIS 根据法定要求（例如，根据劳动和社会保障法、津贴、税务或报告义务、监管义务、网络安全义务、与监管机构的合作义务或法定保留期限）处理员工个人数据，以便履行作为雇主或委托人的合同责任。</p> | <p>GDPR 第 6.1.c 条 中国个人信息保护法第 13.(3) 条</p> |
| <p>在收集个人数据时，FIS 可能会征求个人的同意。如果 FIS 要求某人同意将其个人数据用于特定目的，相关人员可随时撤销同意，我们会告知如何撤销同意。</p> | <p>GDPR 第 6.1.a 条 中国个人信息保护法第 13.(1) 条</p> |

处理敏感个人数据的法律依据：

对于特殊类别的个人数据，FIS 仅会在适用法律允许的情况下和以下情况下处理此类数据：

| | |
|---|---|
| <p>根据适用法律，在获得明确同意的情况下进行特定活动</p> | <p>GDPR 第 9.2.a 条 中国个人信息保护法第 29 条</p> |
| <p>经父母责任人同意（针对 16 岁以下学生）</p> | <p>GDPR 第 8.1 条 中国个人信息保护法第 31 条</p> |
| <p>行使基于雇佣或其他合同关系的权利，遵循社会保障或社会保护法的规定，根据集体协议的授权进行处理，进行预防性或职业医学检查，或对工作能力进行评估</p> | <p>GDPR 第 9.2.b 条</p> |

员工隐私声明

| | |
|---|-----------------------|
| <p>为了确立、行使或捍卫法律主张，或遵守司法机关以司法身份作出的指示或要求。</p> | <p>GDPR 第 9.2.f 条</p> |
| <p>对于涉及刑事定罪和犯罪的个人数据，FIS 仅在适用（当地）法律允许的情况下才会进行处理。</p> | <p>GDPR 第 10 条</p> |