2018–2022年涉数字经济犯罪案件司法白皮书系列

# 企业数据合规指引
# 个人信息保护指引

上海市杨浦区人民法院
上海市杨浦区人民检察院

# 目　录

# 企业数据合规指引

## 1. 目的

为引导企业加强数据合规管理，保护个人信息，保障数据安全，规范数据处理活动，根据《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规（以下统称为数据法规），制定本指引。

## 2. 数据分类分级保护

企业应当建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度进行分类分级，针对不同类别级别的数据采取相应的保护措施。

## 3. 数据权益保障

鼓励数据处理者按照《上海市数据条例》的规定开发和利用数据资源。数据处理者依法在数据处理活动中形成的法定或者约定的财产权益，以及在数字经济发展中有关数据创新活动取得的合法财产权益受法律保护。

## 4. 数据合规管理体系

### 4.1 合规责任人

企业的最高管理者是数据合规的第一责任人。最高管理者应当承担以下职责：

1）分配足够和适当的资源来建立、发展、实施、评估、维护和改进数据合规管理体系；

2）确保建立举报数据违规的有效机制；

3）确保战略和运营目标与履行数据合规义务之间的一致性；

4）建立和维护问责机制，包括纪律处分和后果；

5）确保将数据合规落实情况和效果纳入企业内部人员绩效考核体系。

4.2 数据合规管理部门

鼓励各类企业设置专门的数据合规管理部门，或者将数据合规管理职能融入现有的企业合规管理体系，但是不建议由法务部门履行合规管理职能。企业应当向数据合规管理部门负责人提供足够的授权、人力、财力来支持数据合规管理体系的运行。一般由董事会直接设立企业合规部门，下设数据合规管理部门等各类专业合规部门。数据合规管理部门应履行以下职责：

1）制定数据合规管理整体方针策略，协调建立数据合规技术保障措施，牵头做好数据风险识别、风险评估、风险处置等工作；

2）制定、完善数据合规计划，并推动其有效实施；

3）审核评估企业的经营管理和业务行为，确保企业与供应商、代理商、经销商、关联企业、分支机构的业务活动，以及处理个人信息等活动符合数据法规的要求，并制定数据风险应对措施；

4）组织或协助管理部门、业务部门等开展数据合规教育培训，并向管理层和各部门员工提供数据合规咨询；

5）建立数据合规举报记录台账，对数据合规举报制定调查方案并开展调查；

6）推动将数据合规责任纳入企业岗位职责和员工绩效考核评价体系，培养数据合规文化；

7）持续关注国内和业务所涉国家（地区）数据法规的发展动态，及时提供数据合规建议。

数据合规管理部门应加强与业务部门的分工协作。相关业务部门应主动进行日常数据合规管理工作，识别业务范围内的合规要求，制定并落实业务管理制度和风险防范措施，配合数据合规管理部门进行合规风险审查、评估和调查、处置、整改工作。

数据合规管理部门应与其他具有合规管理职能的监督部门（如法务部门、审计部门、监察部门等）建立明确的合作和信息交流机制，加强协调配合。

企业应积极与数据监管部门建立沟通渠道，了解数据监管部门期望的数据合规体系，并制定符合其要求的数据合规制度；对于复杂或专业性强且存在重大数据风险的事项，可以向数据监管部门咨询；面对数据监管部门的调查，企业应积极沟通并予以配合。

4.3 数据合规计划

数据合规部门负责人应结合企业自身的经营范围、行业特征、监管政策、风险识别等因素制定并不断完善数据

合规计划。数据合规计划应当根据企业内部环境和外部环境的变化不断调整，以帮助企业应对各种风险的挑战。

**5. 数据风险识别**

1）风险识别

企业开展数据合规管理应当准确识别风险。常见的数据风险包括数据全生命周期各阶段中可能存在的未授权访问、数据滥用、数据泄漏等风险，以及侵犯个人信息、非法获取计算机信息系统数据、传播违法信息、侵犯知识产权、非法跨境提供数据等刑事犯罪风险，企业应根据识别出的风险评估相关经营管理和业务行为是否合规。

2）禁止从事的数据活动

企业及其员工开展数据处理活动应当遵守法律、行政法规，尊重社会公德和伦理，不得从事以下活动：

a）危害国家安全、荣誉和利益，泄露国家秘密和工作秘密；

b）侵害他人人格权、知识产权和其他合法权益等；

c）通过窃取或者以其他非法方式获取数据；

d）非法出售或者非法向他人提供数据；

e）制作、发布、复制、传播违法信息；

f）法律、行政法规禁止的其他行为。

任何个人和组织知道或者应当知道他人从事前款活动的，不得为其提供技术支持、工具、程序和广告推广、支付结算等服务。

**6. 数据风险评估与处置**

1）风险评估

企业在识别数据风险内容的基础上，可根据自身经营规模、组织体系、业务内容以及市场环境，分析和评估数据风险的来源、发生的可能性、后果的严重性等，并对数据风险进行分级。

数据合规部门负责人应当根据风险评估结果对不同职级、不同工作范围的管理层与员工进行风险提示，降低管理层和员工的违法犯罪风险。

2）风险处置机制

企业应建立健全数据安全事件应急预案与风险处置机制，对识别和评估的各类数据风险设置恰当的控制和应对措施来降低风险，必要时停止相关风险行为。安全事件涉嫌犯罪的，应当及时向公安机关报案。

3）立即停止违法行为

经评估发现可能已经发生数据违法行为，或者数据监管部门已立案并启动调查程序的，企业应当立即停止违法行为并与执法机构合作。

4）积极应对数据监管部门的调查

当企业受到数据监管部门调查时，应通知管理层、法务负责人、数据合规负责人和相关业务工作负责人等，按照企业内部受调查操作流程妥善应对,进行内部初步调查，分析相关法律法规并评估数据违法行为成立的可能性与法律后果。企业应积极配合数据监管机构调查。不得拒绝提供有关材料、信息，或者提供虚假材料、信息，或者隐匿、

销毁、转移证据，或者有其他拒绝、阻碍调查的行为。

5）投诉举报渠道

数据处理者应当建立便捷的数据安全投诉举报渠道，及时受理、处置数据安全投诉举报。

数据处理者应当公布接受投诉、举报的联系方式、责任人信息,每年公开披露受理和收到的数据安全投诉数量、投诉处理情况、平均处理时间情况，接受社会监督。

**7. 数据合规运行与保障**

1）合规咨询

企业可建立数据合规咨询机制，管理层和各部门员工在工作中可以向数据合规管理部门咨询数据合规问题。数据合规管理部门应当不断学习、提升合规管理水平，也可以同外部机构开展数据合规咨询合作。

2）发现机制

数据合规管理部门可以通过设置日常的流程监控、内部审核、重点核查以及定期评查等方式发现企业及员工的违规行为，并及时按照合规计划采取相应的处置措施。数据合规管理部门应定期向合规负责人汇报数据合规管理情况。当发生可能给企业带来重大数据合规风险的违规行为时，应当及时向合规负责人汇报，并提出相应的解决方案。

3）举报机制

员工根据合规计划可以实名或者匿名通过内部举报系统举报数据违规行为，并严格保护实名举报者和匿名举报者不受打击和报复，尤其是保护匿名举报者的个人信息安

全。

4）激励和纪律

企业应当建立数据合规考核机制，数据合规考核结果作为企业绩效考核的重要依据，与员工的评优评先、职务任免、职务晋升以及薪酬待遇等挂钩。对于严格遵守数据合规的管理层和员工，制定适当的激励措施使合规计划得到一致遵守和执行。对于不严格执行甚至违反合规计划的管理层和员工，采取适当的纪律措施进行惩戒，并根据违规程度采取不同的风险处置措施。

5）培训与承诺

数据合规管理部门应当建立培训机制，定期为管理层、员工培训数据合规，使其充分了解数据法规、数据合规计划、岗位角色与职责等。

6）数据合规管理信息化建设

企业可通过数据合规管理信息化建设，并运用大数据分析等工具，加强对经营管理行为中的数据合规的实时监控和风险分析。

7）数据合规文化培育

鼓励企业将数据合规文化作为企业文化建设的重要内容，践行合规经营的价值观，不断增强员工的数据合规意识。鼓励行业协会在本行业内积极倡导数据合规文化，强化行业的数据合规意识。

**8. 基本概念**

1）数据，是指任何以电子或者其他方式对信息的记录。

2）数据合规，是指企业及其员工的经营管理行为符合个人信息保护、网络安全、数据安全等数据法规的要求；

3）数据合规管理，是指以预防和降低涉数据违法犯罪为目的，以企业及其员工经营管理行为为对象，开展包括合规管理体系、风险识别、风险评估与处置、合规运行与保障等有组织、有计划的管理活动；

4）数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

## 附：企业可参考的相关法律法规与标准

| 序号 | 类型 | 层级 | 名 称 |
|---|---|---|---|
| 1 | 数据安全 | 法律 | 《国家安全法》 |
| 2 | | 法律 | 《网络安全法》 |
| 3 | | 法律 | 《数据安全法》 |
| 4 | | 司法解释 | 《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》 |
| 5 | | 行政法规 | 《网络数据安全管理条例》（征求意见稿） |
| 6 | | 部门规章 | 《网络安全审查办法》 |
| 7 | | 部门规范性文件 | 《网络数据安全标准体系建设指南》（征求意见稿） |
| 8 | | 标准 | 《网络数据处理安全规范》（征求意见稿） |
| 9 | 重要数据保护 | 标准 | 《重要数据识别指南》（征求意见稿） |
| 10 | | 标准 | 《基础电信企业重要数据识别指南》2019-0217T-YD CCSA 草案 |
| 11 | 个人信息保护 | 法律 | 《个人信息保护法》 |
| 12 | | 标准 | 《信息安全技术个人信息安全规范》（GB/T 35273—2020） |
| 13 | 数据出境安全评估 | 部门规章 | 《数据出境安全评估办法》（征求意见稿） |
| 14 | | 标准 | 《信息安全技术 数据出境安全评估指南》（征求意见稿） |

| 序号 | 类型 | 层级 | 名 称 |
| --- | --- | --- | --- |
| 15 | 电信领域 | 部门规章 | 《工业和信息化领域数据安全管理办法（试行）》（征求意见稿） |
| 16 | | 标准 | 《基础电信企业数据分类分级方法》 |
| 17 | | 标准 | 《基础电信企业重要数据识别指南》 |
| 18 | | 标准 | 《电信网和互联网数据安全评估规范》 |
| 19 | | 标准 | 《电信网和互联网数据安全通用要求》 |
| 20 | 金融领域 | 标准 | 《金融数据安全数据安全分级指南》(JR/T 0197—2020) |
| 21 | | 标准 | 《金融数据安全 数据生命周期安全规范》(JR/T 0223—2021) |
| 22 | | 标准 | 《金融数据安全 数据安全评估规范》（征求意见稿） |
| 23 | | 标准 | 《金融数据跨境安全要求》（征求意见稿） |
| 24 | | 标准 | 《证券期货业数据分类分级指引》(JR/T 0158-2018) |
| 25 | 汽车领域 | 部门规章 | 《汽车数据安全管理若干规定（试行）》 |
| 26 | | 部门工作文件 | 《工业和信息化部关于加强车联网网络安全和数据安全工作的通知》 |
| 27 | 医疗领域 | 部门规范性文件 | 《国家健康医疗大数据标准、安全和服务管理办法（试行）》 |
| 28 | | 标准 | 《信息安全技术健康医疗数据安全指南》 |

# 个人信息保护指引

## 1. 目的

为了更好的帮助企业做好个人信息保护工作，识别个人信息处理中可能存在的刑事法律风险，特制定本指引。

## 2. 术语和定义

1）个人信息：以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。本指引下个人信息包括企业员工、客户（客户包括供应商、自然人和企业客户、合作伙伴等）以及生产经营中处理的其他个人信息。

2）敏感个人信息：一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

3）个人信息的处理：包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

4）个人信息处理者：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。

5）自动化决策：通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

6）去标识化：个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

7）匿名化：个人信息经过处理无法识别特定自然人且不能复原的过程。

**3. 处理个人信息的基本原则**

1）正当诚信原则：处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

2）最小必要原则：处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

3）公开透明原则：处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

4）质量原则：处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

5）安全原则：个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

6）合法性原则：任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

**4. 处理个人信息的合法前提**

处理个人信息前，应向信息主体告知个人信息处理者名称、联系方式、处理目的、处理方式，处理的个人信息种类、保存期限等，并获得信息主体同意。

符合以下情形的，无需取得信息主体同意：

1）为订立、履行个人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《中华人民共和国个人信息保护法》规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

6）法律、行政法规规定的其他情形。

针对敏感个人信息，应采取更为严格的个人信息保护措施，包括但不限于：

1）处理敏感个人信息前应取得个人的单独同意；

2）应向个人告知个人信息处理者名称、联系方式、处理目的、处理方式，处理的个人信息种类、保存期限、处理敏感个人信息的必要性以及对个人权益的影响；

3）处理敏感个人信息前，应进行个人信息保护影响评估，并对处理情况进行记录；

4）处理不满十四周岁未成年人个人信息的，应取得未成年人的父母或者其他监护人的同意，并制定专门的个人信息处理规则。

**5. 收集**

直接收集个人信息的，应当符合前述第 4 条的要求，从第三方处接受、共享、收集个人信息的，应当确认该第三方有权提供且个人信息获取方式合法正当；不得通过非法买卖、交换、窃取等方式获取个人信息。

通过自动化方式收集个人信息的，例如爬虫等方式，应当确保收集权限，不得采取绕开访问控制、反爬虫等措施，应当合理设置相关参数并采取合理管理，避免对网络造成干扰或者破坏等后果。

通过业务合作等合法方式使用个人信息的，不得通过缓存等方式非法留存。

**6. 提供与共享**

向第三方提供、共享个人信息前，应当采取以下合规措施：

1）向个人信息主体告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类；

2）获得信息主体单独同意；

3）事前进行个人信息保护影响评估，并对处理情况进行记录；

4）不得通过交易、交换、买卖等方式向第三方提供、共享个人信息。

**7. 存储与传输**

存储个人信息的期限需遵从以下原则：

1）法律法规有明确要求的，遵照法律法规要求；

2）法律法规无明确要求的，根据双方合同约定（该约定仍应当符合最小必要等基本原则）；

3）双方无约定的，为实现个人信息处理目的所必要的最短时间；

4）涉及员工个人信息存储的，建议一般按照员工离职后 3 年（参考诉讼时效）为时限。

传输个人信息时，应采取必要的安全措施，如加密等；应当对存储和传输个人信息的信息系统按照网络安全等级保护制度要求，履行安全保护义务，保障信息系统免受干扰、破坏或者未经授权的访问，防止个人信息泄露或者被窃取、篡改。

**8. 自动化决策**

在使用基于个人信息的自动化决策时，应履行以下义务：

1）保证决策的透明度和结果公平、公正，不对个人在交易价格等交易条件上实行不合理的差别待遇；

2）提供不针对个人信息主体特征的选项，或者向个人提供便捷的拒绝方式；

3）通过自动化决策方式作出对个人权益有重大影响的决定时，企业应根据信息主体要求予以说明，并保障信息主体有权拒绝自动化决策的方式作出决定；

4）进行相关个人信息保护影响评估并进行记录。

**9. 提供服务**

通过自动化决策或者其他涉及使用个人信息提供服务时，应当对服务购买和接收方行为保持密切关注，发现服务接收方可能实施犯罪或者出现下列异常情形的，应当及时采取有关措施，必要时报告主管部门：

1）交易价格或者方式明显异常的；

2）监管部门告知服务接收方存在异常情形的；

3）接到对服务接收方举报的；

4）其他异常情形的。

**10. 公开披露**

如果需要公开所处理的个人信息的，应履行以下义务：

1）公开前取得个人单独同意；

2）公开前对个人信息保护影响进行评估，并对处理情况进行记录。

**11. 出境**

确因业务或其他合理目的需要，将个人信息传输至境外的，应履行以下合规义务：

1）出境前通过同意函等形式获得个人单独同意；

2）向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使《中华人民共和国个人信息保护法》规定权利的方式和程序等事项；

3）事前进行个人信息保护影响评估，并对处理情况进行记录；

4）符合以下条件处理个人信息的，应申请安全评估：

a）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；

b）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；

c）国家网信部门规定的其他需要申报数据出境安全评估的情形。

5）不符合前述第 4）任一情形的，应采取个人信息保护认证或标准合同方式履行个人信息保护义务。

**12. 个人信息保护影响评估及合规审计**

12.1 有下列情形之一的，事前进行个人信息保护影响评估，并对处理情况进行记录：

1）处理敏感个人信息；

2）利用个人信息进行自动化决策；

3）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

4）向境外提供个人信息；

5）其他对个人权益有重大影响的个人信息处理活动。

12.2 个人信息保护影响评估应当包括下列内容：

1）个人信息的处理目的、处理方式等是否合法、正当、必要；

2）对个人权益的影响及安全风险；

3）所采取的保护措施是否合法、有效并与风险程度相

适应；

4）针对个人信息出境的个人信息保护影响评估，应遵照《个人信息出境标准合同备案指南》要求开展。

12.3 个人信息保护影响评估报告和处理情况记录应当至少保存三年。

12.4 定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。审计的方式既可以由企业自行开展，也可聘请外部机构协助开展。

## 13. 事件处置

13.1 事前

1）应制定个人信息安全事件应急预案，并根据法律法规要求、监管要求及时更新内容；

2）应根据本预案定期（至少每年一次）/ 不定期组织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，确保本预案的有效性；

3）培训、演练工作完成前后，应当做好培训、演练记录并存档。

13.2 事中

1）安全事件发生后，企业应立即采取补救措施，可采取包括但不限于更改口令、回收权限、断开网络连接等方式。

2）对于个人信息安全事件，个人信息安全事件响应团队评估后确认属于个人信息安全事件的，应当立即通知主管部门和相关信息主体。通知应当包括下列事项：

a）发生或者可能发生个人信息泄露、篡改、丢失的信

息种类、原因和可能造成的危害；

b）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；

c）个人信息处理者的联系方式。

企业采取措施能够有效避免信息泄露、篡改、丢失造成危害的，可以不通知个人。

需要通知个人的，应及时将相关情况以邮件、信函、电话、推送通知等方式告知，难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。

13.3 事后回顾和总结

安全事件处置结束后，企业应及时总结事件并对应急预案中需要改进的部分认真研判，根据需要，对应急预案及相关管理制度进行修订、发布和宣讲，以提高个人信息安全事件应急响应能力。

**14. 监管部门调查与处置**

对于监管部门的调查、处罚、责令整改等，应当积极应对，及时消除违法事项，落实整改措施。对于因客观原因无法及时整改、落实的，应当提出整改计划并向监管部门汇报沟通。

**15. 管理制度**

15.1 应建立和完善个人信息保护管理制度，合理确定相关岗位及人员的个人信息处理操作权限。

15.2 应定期对员工进行个人信息保护相关教育和培训，并做好相关培训记录。

## 附：个人信息示例

| | |
|---|---|
| 个人基本资料 | 个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮箱地址等 |
| 个人身份信息 | 身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等 |
| 个人生物识别信息 | 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等 |
| 网络身份标识信息 | 个人信息主体账号、IP 地址、数字证书等 |
| 个人健康生理信息 | 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、既往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况产生的相关信息，及体重、身高、肺活量等 |
| 个人教育工作信息 | 个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等 |
| 个人财产信息 | 银行账号、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息 |
| 个人通信信息 | 通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等 |
| 联系人信息 | 通讯录、好友列表、群列表、电子邮件地址列表等 |
| 个人上网记录 | 指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等 |

| | |
|---|---|
| 个人常用设备信息 | 指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/android、ID/IDFA/OPENUDID/GUID、SIM 卡、IMSI 信息等）等在内的描述个人常用设备基本情况的信息 |
| 个人位置信息 | 包括行踪轨迹、精准定位信息、住宿信息、经纬度等 |
| 其他信息 | 婚史、宗教信仰、性取向、未公开的违法犯罪记录等 |

## 附：敏感个人信息

| | |
|---|---|
| 个人财产信息 | 银行账号、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息 |
| 个人健康生理信息 | 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、既往病史、诊治情况、家族病史、现病史、传染病史等 |
| 个人生物识别信息 | 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等 |
| 个人身份信息 | 身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等 |
| 其他信息 | 性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等 |

上海市杨浦区人民法院

上海市杨浦区人民检察院