软通动力个人隐私政策

版本：V 1.0

1 导言

1.1 目的

为规范软通动力在个人信息方面的管理，满足国家相关法律法规的要求，同时有效保护个人信息资产，依据相关国家标准规范制定本制度。

1.2 范围

本制度适用于软通动力信息技术（集团）股份有限公司及其中国境内（不含港澳台地区）的分公司、全资子公司以及持股 50%以上的控股子公司及其分、子公司。

1.3 定义

1.3.1 个人信息：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。

注 1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：对用户信息进行分析加工、用户画像、特征标签，能够单独或与其他信息结合识别个人的，属于个人信息。

1.3.2 个人敏感信息：一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

1.3.3 个人信息主体：个人信息所标识或者关联的自然人。

1.3.4 个人信息控制者：有能力决定个人信息处理目的、方式等的组织或个人。

1.3.5 个人信息处理者：代表并按照个人信息控制者的指示处理个人信息的组织或个人。

1.3.6 收集：获得个人信息的控制权的行为。

注 1：包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人信息等行为。

注 2：如果产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集。例如，离线导航软件在终端获取个人信息主体位置信息后，如果不回传至软件提供者，则不属于个人信息主体位置信息的收集。

1.3.7 明示同意：个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。

注：肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

1.3.8 授权同意：个人信息主体对其个人信息进行特定处理作出明确授权的行为。

注：包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权（如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。

1.3.9 用户画像：通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

1.3.10 公开披露：向社会或不特定人群发布信息的行为。

1.3.11 匿名化：通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

1.3.12 去标识化：通过对个人信息的技术处理，使其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。

注：去标识化建立在个体基础之上，保留了个体颗粒度，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。

1.3.13 个性化展示：基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。

1.3.14 业务功能：满足个人信息主体的具体使用需求的服务类型。

注：如地图导航、网络约车、即时通讯、网络社区、网络支付、新闻资讯、网上购物、快递配送、交通票务等。

2 个人信息安全基本原则

开展个人信息处理活动应遵循合法、正当、必要的原则，具体包括：

a) 权责一致——采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任；

b) 目的明确——具有明确、清晰、具体的个人信息处理目的；

c) 选择同意——向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意；

d) 最小必要——只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息；

e) 公开透明——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督；

f) 确保安全——具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性；

g) 主体参与——向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。

3 个人信息处理要求

3.1 个人信息的收集

3.1.1 收集个人信息的合法性

a) 不应以欺诈、诱骗、误导的方式收集个人信息；

b) 不应隐瞒产品或服务所具有的收集个人信息的功能；

c) 不应从非法渠道获取个人信息。

3.1.2 收集个人信息的最小必要

a) 收集的个人信息的类型应与实现产品或服务的业务功能有直接关联；直接关联是指没有上述个人信息的参与，产品或服务的功能无法实现；

b) 自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；

c) 间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

3.1.3 多项业务功能的自主选择

当产品或服务提供多项需收集个人信息的业务功能时，不应违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求。要求包括：

a) 不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求；

b) 应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。应仅在个人信息主体开启该业务功能后，开始收集个人信息；

c) 关闭或退出业务功能的途径或方式应与个人信息主体选择使用业务功能的途径或方式同样方便。个人信息主体选择关闭或退出特定业务功能后，应停止该业务功能的个人信息收集活动；

d) 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应频繁征求个人信息主体的授权同意；

e) 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应暂停个人信息主体自主选择使用的其他业务功能，或降低其他业务功能的服务质量；

f) 不得仅以改善服务质量、提升使用体验、研发新产品、增强安全性等为由，强制要求个人信息主体同意收集个人信息。

3.1.4 收集个人信息时的授权同意

a) 收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体的授权同意；

注：如产品或服务仅提供一项收集、使用个人信息的业务功能时，可通过个人信息保护政策的形式，实现向个人信息主体的告知；产品或服务提供多项收集、使用个人信息的业务功能的，除个人信息保护政策外，宜在实际开始收集特定个人信息时，向个人信息主体提供收集、使用该个人信息的目的、方式和范围，以便个人信息主体在作出具体的授权同意前，能充分考虑对其的具体影响。

b) 收集个人敏感信息前，应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示；

c) 收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意；

注：个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

d) 收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意；

e) 间接获取个人信息时：

1) 应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；

2) 应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露、删除等；

3) 如开展业务所需进行的个人信息处理活动超出已获得的授权同意范围的，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意，或通过个人信息提供方征得个人信息主体的明示同意。

3.1.5 征得授权同意的例外

以下情形中，个人信息控制者收集、使用个人信息不必征得个人信息主体的授权同意：

a) 与个人信息控制者履行法律法规规定的义务相关的；

b) 与国家安全、国防安全直接相关的；

c) 与公共安全、公共卫生、重大公共利益直接相关的；

d) 与刑事侦查、起诉、审判和判决执行等直接相关的；

e) 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授权同意的；

f) 所涉及的个人信息是个人信息主体自行向社会公众公开的；

g) 根据个人信息主体要求签订和履行合同所必需的；

注：个人信息保护政策的主要功能为公开个人信息控制者收集、使用个人信息范围和规则，不宜将其视为合同。

h) 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；

i) 维护所提供产品或服务的安全稳定运行所必需的，如发现、处置产品或服务的故障；

j) 个人信息控制者为新闻单位，且其开展合法的新闻报道所必需的；

k) 个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的。

3.2 个人信息的存储

3.2.1 个人信息存储时间最小化

a) 个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，法律法规另有规定或者个

人信息主体另行授权同意的除外；

b) 超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理。

3.2.2 去标识化处理

收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

3.2.3 个人敏感信息的传输和存储

对个人信息控制者的要求包括：

a) 传输和存储个人敏感信息时，应采用加密等安全措施；

注：采用密码技术时宜遵循密码管理相关国家标准。

b) 个人生物识别信息应与个人身份信息分开存储；

c) 原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于：

1) 仅存储个人生物识别信息的摘要信息；

2) 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；

3) 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

注 1：摘要信息通常具有不可逆特点，无法回溯到原始信息。

注 2：个人信息控制者履行法律法规规定的义务相关的情形除外。

3.2.4 个人信息控制者停止运营

当个人信息控制者停止运营其产品或服务时，应：

a) 及时停止继续收集个人信息；

b) 将停止运营的通知以逐一送达或公告的形式通知个人信息主体；

c) 对其所持有的个人信息进行删除或匿名化处理。

3.3 个人信息的使用

3.3.1 个人信息访问控制措施

a) 对被授权访问个人信息的人员，应建立最小授权的访问控制策略，使其只能访问职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限；

b) 对个人信息的重要操作设置内部审批流程，如进行批量修改、拷贝、下载等重要操作；

c) 对安全管理人员、数据操作人员、审计人员的角色进行分离设置；

d) 确因工作需要，需授权特定人员超权限处理个人信息的，应经个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册；

e) 对个人敏感信息的访问、修改等操作行为，宜在对角色权限控制的基础上，按照业务流程的需求触发操作授权。例如，当收到客户投诉，投诉处理人员才可访问该个人信息主体的相关信息。

3.3.2 个人信息的展示限制

涉及通过界面展示个人信息的（如显示屏幕、纸面），宜对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。例如，在个人信息展示时，防止内部非授权人员及个人信息主体之外的其他人员未经授权获取个人信息。

3.3.3 个人信息使用的目的限制

a) 使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意；

注：将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，需对结果中所包含的个人信息进行去标识化处理。

b) 如所收集的个人信息进行加工处理而产生的信息，能够单独或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，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围。

注：加工处理而产生的个人信息属于个人敏感信息的，对其处理需符合对个人敏感信息的要求。

3.3.4 用户画像的使用限制

a) 用户画像中对个人信息主体的特征描述，不应：

1) 包含淫秽、色情、赌博、迷信、恐怖、暴力的内容；

2) 表达对民族、种族、宗教、残疾、疾病歧视的内容。

b) 在业务运营或对外业务合作中使用用户画像的，不应：

1) 侵害公民、法人和其他组织的合法权益；

2) 危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。

c) 除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。例如，为准确评价个人信用状况，可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户画像。

3.3.5 个性化展示的使用

a) 在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容；

注：显著区分的方式包括但不限于：标明“定推”等字样，或通过不同的栏目、版块、页面分别展示等。

b) 在向个人信息主体提供电子商务服务的过程中，根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项；

注：基于个人信息主体所选择的特定地理位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和

搜索结果排序，则属于不针对其个人特征的选项。

c) 在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应：

1) 为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项；

2) 当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。

d) 在向个人信息主体提供业务功能的过程中使用个性化展示的，宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关性程度的能力。

3.3.6 基于不同业务目的所收集个人信息的汇聚融合

a) 应遵守 4.3.3 的要求；

b) 应根据汇聚融合后个人信息所用于的目的，开展个人信息安全影响评估，采取有效的个人信息保护措施。

3.3.7 信息系统自动决策机制的使用

个人信息控制者业务运营所使用的信息系统，具备自动决策机制且能对个人信息主体权益造成显著影响的（例如，自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等），应：

a) 在规划设计阶段或首次使用前开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b) 在使用过程中定期（至少每年一次）开展个人信息安全影响评估，并依评估结果改进保护个人信息主体的措施；

c) 向个人信息主体提供针对自动决策结果的投诉渠道，并支持对自动决策结果的人工复核。

3.4 个人信息的委托处理、共享、转让、公开披露

3.4.1 委托处理

个人信息控制者委托第三方处理个人信息时，应符合以下要求：

a) 个人信息控制者作出委托行为，不应超出已征得个人信息主体授权同意的范围或应遵守4.1.6所列情形；

b) 个人信息控制者应对委托行为进行个人信息安全影响评估，确保受委托者达到应有的数据安全能力要求；

c) 受委托者应：

1) 严格按照个人信息控制者的要求处理个人信息。受委托者因特殊原因未按照个人信息控制者的要求处理个人信息的，应及时向个人信息控制者反馈；

2) 受委托者确需再次委托时，应事先征得个人信息控制者的授权；

3) 协助个人信息控制者响应个人信息主体基于 5.1~5.6 提出的请求；

4) 受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件的，应及时向个人信息控制者反馈；

5) 在委托关系解除时不再存储相关个人信息。

d) 个人信息控制者应对受委托者进行监督，方式包括但不限于：

1) 通过合同等方式规定受委托者的责任和义务；

2) 对受委托者进行审计。

e) 个人信息控制者应准确记录和存储委托处理个人信息的情况；

f) 个人信息控制者得知或者发现受委托者未按照委托要求处理个人信息，或未能有效履行个人信息安全保护责任的，应立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险。必要时个人信息控制者应终止与受委托者的业务关系，并要求受委托者及时删除从个人信息控制者获得的个人信息。

3.4.2 个人信息共享、转让

个人信息控制者共享、转让个人信息时，应充分重视风险。共享、转让个人信息，非因收购、兼并、重组、破产原因的，应符合以下要求：

a) 事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b) 向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果，并事先征得个人信息主体的授权同意。共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别或者关联个人信息主体的除外；

c) 共享、转让个人敏感信息前，除 b）中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息类型、数据接收方的身份和数据安全能力，并事先征得个人信息主体的明示同意；

d) 通过合同等方式规定数据接收方的责任和义务；

e) 准确记录和存储个人信息的共享、转让情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等；

f) 个人信息控制者发现数据接收方违反法律法规要求或双方约定处理个人信息的，应立即要求数据接收方停止相关行为，且采取或要求数据接收方采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险；必要时个人信息控制者应解除与数据接收方的业务关系，并要求数据接收方及时删除从个人信息控制者获得的个人信息；

g) 因共享、转让个人信息发生安全事件而对个人信息主体合法权益造成损害的，个人信息控制者应承担相应的责任；

h) 帮助个人信息主体了解数据接收方对个人信息的存储、使用等情况，以及个人信息主体的权利，例如，访问、更正、删除、注销账户等；

i) 个人生物识别信息原则上不应共享、转让。因业务需要，确需共享、转让的，应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。

3.4.3 收购、兼并、重组、破产时的个人信息转让

当个人信息控制者发生收购、兼并、重组、破产等变更时，对个人信息控制者的要求包括：

a) 向个人信息主体告知有关情况；

b) 变更后的个人信息控制者应继续履行原个人信息控制者的责任和义务，如变更个人信息使用目的时，应重新取得个人信息主体的明示同意；

c) 如破产且无承接方的，对数据做删除处理。

3.4.4 个人信息公开披露

个人信息原则上不应公开披露。个人信息控制者经法律授权或具备合理事由确需公开披露时，应符合以下要求：

a) 事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b) 向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意；

c) 公开披露个人敏感信息前，除 b）中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息的内容；

d) 准确记录和存储个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等；

e) 承担因公开披露个人信息对个人信息主体合法权益造成损害的相应责任；

f) 不应公开披露个人生物识别信息；

g) 不应公开披露我国公民的种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果。

3.4.5 共享、转让、公开披露个人信息时事先征得授权同意的例外

以下情形中，个人信息控制者共享、转让、公开披露个人信息不必事先征得个人信息主体的授权同意：

a) 与个人信息控制者履行法律法规规定的义务相关的；

b) 与国家安全、国防安全直接相关的；

c) 与公共安全、公共卫生、重大公共利益直接相关的；

d) 与刑事侦查、起诉、审判和判决执行等直接相关的；

e) 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授权同意的；

f) 个人信息主体自行向社会公众公开的个人信息；

g) 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。

3.4.6 共同个人信息控制者

对个人信息控制者的要求包括：

a) 当个人信息控制者与第三方为共同个人信息控制者时，个人信息控制者应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向个人信息主体明确告知；

b) 如未向个人信息主体明确告知第三方身份，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，个人信息控制者应承担因第三方引起的个人信息安全责任。

注：如个人信息控制者在提供产品或服务的过程中部署了收集个人信息的第三方插件（例如，网站经营者与在其网页或应用程序中部署统计分析工具、软件开发工具包 SDK、调用地图 API 接口），且该第三方并未单独向个人信息主体征得收集个人信息的授权同意，则个人信息控制者与该第三方在个人信息收集阶段为共同个人信息控制者。

3.4.7 第三方接入管理

当个人信息控制者在其产品或服务中接入具备收集个人信息功能的第三方产品或服务且不适用4.4.1和4.4.6时，个人信息控制者将采取以下措施保障个人信息安全：

a) 严格审核与管理接入方：对拟接入的第三方服务进行必要的合规审查与安全评估，确保其具备相应的个人信息保护能力，并根据评估结果决定是否接入。

b) 明确安全责任与数据保护义务：通过合同等方式与第三方明确各自的个人信息保护责任，并要求其严

格按照法律法规履行个人信息保护义务。

c) 清晰标识第三方服务来源：当个人使用的功能或内容由第三方提供时，在产品界面中明确进行标识，帮助您知悉信息来源。

d) 确保用户知情与授权：除法律另有规定外，个人信息控制者会要求第三方在收集个人信息前取得个人的明示同意。必要时，个人信息控制者将协助核验其收集方式是否符合要求。

e) 保障用户权益：个人信息控制者会要求第三方建立用户申诉与信息查询机制，确保个人可以便捷地行使查询、更正、删除等个人信息相关权利。

f) 持续监督与管理：对第三方服务的个人信息处理行为进行监督，定期开展技术检测和行为审计。如发现其存在未按约定收集、使用信息的行为，个人信息控制者有权采取暂停或终止接入等措施。

3.4.8 个人信息跨境传输

在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应遵循国家相关规定和相关标准的要求。

4 个人信息主体的权利

4.1 个人信息查询

个人信息控制者应向个人信息主体提供查询下列信息的方法：

a) 其所持有的关于该主体的个人信息或个人信息的类型；

b) 上述个人信息的来源、所用于的目的；

c) 已经获得上述个人信息的第三方身份或类型。

注：个人信息主体提出查询非其主动提供的个人信息时，个人信息控制者可在综合考虑不响应请求可能对个人信息主体合法权益带来的风险和损害，以及技术可行性、实现请求的成本等因素后，作出是否响应的决定，并给出解释说明。

4.2 个人信息更正

个人信息主体发现个人信息控制者所持有的该主体的个人信息有错误或不完整的，个人信息控制者应为其提供请求更正或补充信息的方法。

4.3 个人信息删除

对个人信息控制者的要求包括：

a) 符合以下情形，个人信息主体要求删除的，应及时删除个人信息：

1) 个人信息控制者违反法律法规规定，收集、使用个人信息的；

2) 个人信息控制者违反与个人信息主体的约定，收集、使用个人信息的。

b) 个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止共享、转让的行为，并通知第三方及时删除；

c) 个人信息控制者违反法律法规规定或违反与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。

4.4 个人信息主体撤回授权同意

对个人信息控制者的要求包括：

a) 应向个人信息主体提供撤回收集、使用其个人信息的授权同意的方法。撤回授权同意后，个人信息控制者后续不应再处理相应的个人信息；

b) 应保障个人信息主体拒绝接收基于其个人信息推送商业广告的权利。对外共享、转让、公开披露个人信息，应向个人信息主体提供撤回授权同意的方法。

注：撤回授权同意不影响撤回前基于授权同意的个人信息处理。

4.5 个人信息主体注销账户

对个人信息控制者的要求包括：

a) 通过注册账户提供产品或服务的个人信息控制者，应向个人信息主体提供注销账户的方法，且方法简便易操作；

b) 受理注销账户请求后，需要人工处理的，应在承诺时限内（不超过15个工作日）完成核查和处理；

c) 注销过程如需进行身份核验，要求个人信息主体再次提供的个人信息类型不应多于注册、使用等服务环节收集的个人信息类型；

d) 注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为注销的必要条件等；

注1：多个产品或服务之间存在必要业务关联关系的，例如，一旦注销某个产品或服务的账户，将会导致其他产品或服务的必要业务功能无法实现或者服务质量明显下降的，需向个人信息主体进行详细说明。

注2：产品或服务没有独立的账户体系的，可采取对该产品或服务账号以外其他个人信息进行删除，并切断账户体系与产品或服务的关联等措施实现注销。

e) 注销账户的过程需收集个人敏感信息核验身份时，应明确对收集个人敏感信息后的处理措施，如达成目的后立即删除或匿名化处理等；

f) 个人信息主体注销账户后，应及时删除其个人信息或匿名化处理。因法律规规定需要留存个人信息的，

不能再次将其用于日常业务活动中。

4.6 个人信息主体获取个人信息副本

根据个人信息主体的请求，个人信息控制者宜为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将以下类型个人信息的副本传输给个人信息主体指定的第三方：

a) 本人的基本资料、身份信息；

b) 本人的健康生理信息、教育工作信息。

4.7 响应个人信息主体的请求

对个人信息控制者的要求包括：

a) 在验证个人信息主体身份后，应及时响应个人信息主体基于5.1~5.6提出的请求，应在三十天内或法律法规规定的期限内作出答复及合理解释，并告知个人信息主体外部纠纷解决途径；

b) 采用交互式页面（如网站、移动互联网应用程序、客户端软件等）提供产品或服务的，宜直接设置便捷的交互式页面提供功能或选项，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利；

c) 对合理的请求原则上不收取费用，但对一定时期内多次重复的请求，可视情收取一定成本费用；

d) 直接实现个人信息主体的请求需要付出高额成本或存在其他显著困难的，个人信息控制者应向个人信息主体提供替代方法，以保障个人信息主体的合法权益；

e) 以下情行可不响应个人信息主体基于5.1~5.6提出的请求，包括：

1) 与个人信息控制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) 与刑事侦查、起诉、审判和执行判决等直接相关的；

5) 个人信息控制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授权同意的；

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。

f) 如决定不响应个人信息主体的请求，应向个人信息主体告知该决定的理由，并向个人信息主体提供投诉的途径。

4.8 投诉管理

个人信息控制者应建立投诉管理机制和投诉跟踪流程，并在合理的时间内对投诉进行响应。