ICS

T/CSAC

团　　体　　标　　准

T/CSAC XXXXX—XXXX

隐私计算 删除控制技术要求

Privacy computing ： Technology requirement for deletion control

（征求意见稿）

（本稿完成日期：2024/XX/XX）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国网络空间安全协会发布

隐私计算 删除控制技术要求

1 范围

本文件描述了个人信息删除控制的机制及其安全要求，包含删除通知与确认、副本查找、自动删除与按需删除、删除存证等环节的控制技术要求等。

本文件适用于规范各类组织对个人信息删除处理的控制技术要求，也可为主管监管机构、第三方评估机构等组织对个人信息删除处理进行监督、管理、评估提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性应用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

3.1

个人信息 personal information

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，包含个人信息本身及其衍生信息，不包括匿名化处理后的信息。

[来源：GB/T 35273—2020,3.1,有修改]

3.2

个人信息主体 personal information subject

是指个人信息所识别或者关联的自然人。

[来源：GB/T 35273—2020,3.3]

3.3

隐私信息 private information

能通过信息系统进行处理的敏感个人信息，是个人信息记录中的标识符、准标识符和敏感属性的集合。

注：隐私信息包括个人生物特征信息、银行账号、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。

3.4

删除 delete

采用访问控制、消磁、物理破坏等技术或措施，使得信息不能被访问或被检索，或者从物理上去除了信息并保障其难以恢复的操作。

注：删除包括不能被访问或被检索、全部物理删除或部分物理删除。

[来源：GB/T 35273—2020,3.10,有修改]

3.5

数据恢复 data recovery

通过专门的计算机软件、硬件等技术，从删除对象曾经留存过的存储系统或介质中，重建被删除对象的过程。

3.6

删除对象 deleted object

删除操作的客体。

注：删除对象包括个人信息的正本信息、副本信息、正本信息的一部分、副本信息的一部分，以及正本信息与副本信息的全部或者部分的组合。

3.7

删除等级 delete level

对删除对象可恢复程度和难度的量化分级。

3.8

删除意图 delete intention

是指个人信息主体对自身个人信息何时何地何条件何等级下的删除需求，删除意图包括：删除对象、删除时间、删除空间、删除等级等内容，以及个人信息主体的个性化约束条件。

3.9

删除通知 delete notification

用于指示删除对象关联方如何删除的请求，通知内容包括：删除通知发送者、删除通知接收者、删除对象标识、删除触发条件、删除方式、删除通知确认方式等内容。

3.10

删除指令 delete instructions

基于删除通知构造的、程序可识别可执行的删除命令。

3.11

删除通知发送者 delete notification sender

是指删除通知的发起方（含通知生成）或转发方，删除通知发送者可以为人、组织、设备、程序。

3.12

删除通知接收者 delete notification recipient

是指删除通知的接收方，并将删除通知解析为删除指令，分发给个人信息删除者。删除通知接收者一般为个人或者组织。

3.13

删除通知确认 delete notification confirmation

是指删除通知送达删除通知接收者后，接收者给删除通知发送者反馈的接收确认信息。确认信息包含：删除通知接收者标识、删除对象标识、通知确认时间、通知确认的验证信息等内容。

3.14

删除通知到达验证 delete-notification’s arrival verification

以抗抵赖的方式证明删除通知已经送达删除通知接收者。

3.15

个人信息删除者 personal information remover

对持有的个人信息执行删除操作的实体。

3.16

删除执行反馈 delete execution feedback

是指个人信息删除者执行删除操作后，将删除结果反馈给删除通知接收者，然后由删除通知接收者反馈给删除通知发送者。

3.17

按需删除 on-demand delete

是指删除通知发送者、删除通知接收者、个人信息删除者按照个人信息主体删除意图随时触发的删除操作流程。

3.18

自动删除 automatic delete

是指删除通知发送者、删除通知接收者、个人信息删除者按照个人信息主体预先设置的删除意图或者法律法规的要求，自行触发的删除操作流程。

注：自动删除与按需删除的主要差异在于，按需删除一定包含了个人信息主体的删除意图。

3.19

删除约束条件 delete constraint

是指对删除对象执行的删除操作流程需满足的触发要求、执行要求、反馈要求。

3.20

删除触发条件 trigger conditions for deletion

根据删除意图或者法律法规生成的，一旦匹配即刻触发删除流程的判定条件，包括：时间条件、个人信息流传次数条件、接收到删除通知等。

注：删除触发条件一般包括：删除约束时间、删除约束流转次数、符合删除约束位置、符合删除约束设备、符合删除约束网络、符合删除约束操作、接收到通知、发生违规使用行为、符合指定信息属性、符合删除执行主体。

3.21

多副本信息 multiple copies information

是指同一个人信息存储于不同管理域、信息系统的多拷贝。

3.22

多备份信息 multiple backup information

是指同一个人信息存储于同一个管理域或者同一个信息系统内的多拷贝。

3.23

分散存储信息 distributed storage information

是指同一个人信息拆分后分布式存储于不同存储设备/系统中的部分。

3.24

完备删除 complete delete

是指删除个人信息的正本信息、多副本信息、分散存储信息和多备份信息。

3.25

个人信息处理者 personal information processor

对个人信息进行收集、存储、使用、加工、传输、提供、公开、删除、脱敏、存证与取证等操作的实体。

3.26

个人信息源域 original domain of personal information

是指个人信息主体首次留存个人信息的管理域。

3.27

个人信息传播域 broadcasting domain of personal information

是指个人信息流转过程中由个人信息源域传播到达的管理域。

3.28

删除延伸控制 extended delete control

是指删除意图、删除通知及其确认、删除执行反馈及其验证等删除控制规则的传递应与删除对象传播路径保持一致。

注：传播范围包括：系统内部、跨系统、跨管理域、跨网络等。

4 概述

4.1 删除的目的

保障个人信息，特别是隐私信息，在业务非必要使用时，按照个人信息主体删除意图或者法律法规的要求，进行个人信息删除，以降低个人信息被泄露、非法使用的风险，支撑个人信息主体的删除权和被遗忘权。

4.2 删除的基本原则

个人信息处理者开展个人信息删除处理应遵循及时、透明的原则，具体包括:

a) 按照与个人信息主体的约定或设置，采取技术、人工等手段保障个人信息完备删除；
b) 以明确、易懂与合理的方式向个人信息主体及时告知删除结果，包括：时间、范围、规则等；
c) 存证删除流程的关键状态，并接受监管机构或第三方评估机构审查，保障个人信息可信删除；
d) 由于个人信息未能按照约定及时删除导致个人信息主体合法权益造成损害时，应承担责任。

4.3 删除控制的基本流程

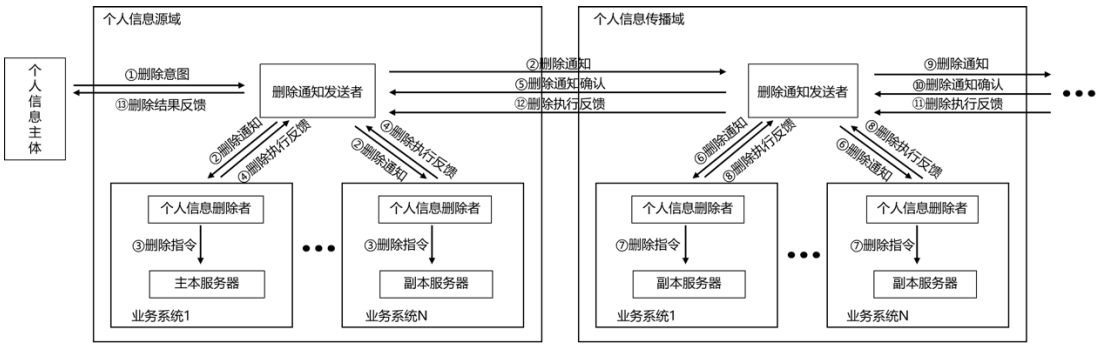

图 1 个人信息删除控制基本流程

如图1所示，个人信息删除控制的基本流程如下：

a) 个人信息主体根据需求设置删除意图，并发送给个人信息源域的删除通知发送者（如图 1 所示步骤 1）；
b) 个人信息源域的删除通知发送者生成删除通知，将删除通知逐级发送给删除对象关联的所有个人信息传播域的删除通知接收者，同时也将删除通知发送给本域且与删除对象关联的所有业务系统的个人信息删除者（如图 1 所示步骤 2、8、9）；
c) 个人信息源域的个人信息删除者收到删除通知后，生成删除指令并要求关联的存储系统执行删除，待删除结束后向本域的删除通知发送者反馈删除结果（如图 1 所示步骤 3、4）；

d) 各个人信息传播域的删除通知接收者收到删除通知后，向上级删除通知发送者反馈删除通知确认信息，并将删除通知发送给本域且与删除对象关联的所有业务系统的个人信息删除者（如图1所示步骤5、6、10）；
e) 各个人信息传播域的个人信息删除者收到删除通知后，生成删除指令并要求关联的存储系统执行删除，待删除结束后向本域的删除通知接收者反馈删除结果（如图1所示步骤7、8）；
f) 各个人信息传播域的删除通知接收者收到删除结果后，向上级删除通知发送者反馈本域的删除结果（如图1所示步骤11、12）；
g) 个人信息源域的删除通知发送者汇总各域的删除结果后，向个人信息主体反馈最终删除结果（如图1所示步骤13）。

5 删除控制通用技术要求

5.1 删除触发

删除触发条件应遵守以下要求：
h) 当个人信息处理目的已实现、无法实现或者为实现处理目的不再必要时；
i) 当个人信息主体注销或终止个人信息处理者提供的产品或服务时；
j) 当个人信息处理者注销或者产品或者业务最终下线、或者保存期限已届满时；
k) 当个人信息主体以书面、邮件或信函等形式提出主观删除意愿时；
l) 当个人撤回同意时；
m) 当行政主管部门、司法裁定等要求删除个人信息时；
n) 依据个人信息收集时个人信息主体的设置或者与个人信息处理者的约定，达到删除条件时；
o) 法律另有要求的除外。

5.2 删除通知与删除通知确认

删除通知与删除通知确认应遵守以下要求：
p) 当个人信息未被设定自动触发的删除条件时，可以通过个人信息主体与个人信息处理者约定的途径发送，发送途径比如：系统消息、程序接口、人工、电话、短信、邮件、信函等；
q) 在个人信息全生命周期中留存个人信息的各个环节，应提供用于接收删除通知的接口或者其他接收方式；
r) 删除通知接收者应以适当的途径反馈删除通知确认信息，反馈途径比如：系统消息、程序接口、人工、电话、短信、邮件、信函等；
s) 删除通知发送者应具有删除通知到达验证能力。

5.3 删除延伸控制

删除延伸控制应遵守以下要求：
t) 删除通知的传递顺序应与个人信息传播的路径相同；
u) 当删除通知在系统内部、跨系统、跨管理域、跨网络传递时，删除通知中的删除控制规则应保持一致，包括删除对象、删除方式等；
v) 当个人信息处理者将个人信息提供给其他个人信息处理者时，应同时传递相应的删除规则，并确保它们履行该删除规则。

5.4 删除方式

依据个人信息的删除等级，个人信息删除者选择不同的删除方式，应遵守以下要求：

w） 可采用物理破坏、化学破坏等方法删除个人信息，具体包括：

1） 物理破坏方法：分解、研磨、粉碎、消磁、压花、滚花磁性存储介质等；

2） 化学破坏方法：溶解、腐蚀、焚化，或者用化学物质剥离磁性存储介质表面信息等。

x） 可采用加密删除、多次覆写删除等方法删除个人信息，具体包括：

1） 加密删除：使用对称或者非对称密码算法对个人信息进行加密存储（比如：硬件内置加密、文件加密、磁盘分区加密、存储设备加密），在执行删除时，对加密密钥执行密钥销毁；

2） 多次覆写删除：在磁性存储介质（比如：磁盘）上执行三次及以上的连续覆写操作，覆盖原有数据。

y） 可采用覆写删除、填充删除、硬件内置删除命令等方法删除个人信息，具体包括：

1） 覆写删除：在磁性存储介质（比如：磁盘）上执行两次及以下的覆写操作，比如：磁盘完全格式化；

2） 填充删除：在固态存储介质（比如：闪存硬盘）上执行擦除操作，比如：闪存硬盘完全格式化；

3） 硬件内置删除命令：使用硬件内置命令，擦除存储介质上的数据，如 ATASecureErase 命令、NVMe Format 命令。

5.5 删除存证

删除过程的存证应遵守以下要求：

z） 应当对删除全流程中的主体、客体、关键步骤、操作、结果等进行存证；

aa） 应采用技术手段，使得存证内容无法被篡改。

5.5.1 删除存证主体

删除存证涉及到的主体包括但不限于：个人信息主体、删除通知发送者、删除通知接收者、个人信息删除者、中心存证系统、本地存证系统、其他业务系统等。

5.5.2 删除存证内容

删除存证内容包括但不限于：删除意图、删除通知、删除通知确认、删除通知发送时间、删除通知接收时间、删除触发、删除方式、删除时间、删除指令、删除算法及参数、删除结果等。

5.5.3 删除存证期限

删除存证期限应遵守以下要求：

bb） 个人信息主体同意后，删除存证可以不再继续保存；

cc） 达到约定的保持期限后，删除存证可以不再继续保存；

dd） 法律另有要求的除外。

6 删除控制技术的实施要求

6.1 按需删除

6.1.1 按需删除概述

按需删除主要是实现个人信息的删除权。个人信息源域的删除通知发送者根据个人信息主体删除意图生成个人信息按需删除通知，并需保证所有关联的个人信息传播域的删除通知接收者能按照按需删除通知完成对删除对象的按需删除，最终整体实现个人信息完备删除。按需删除流程一般应包括以下几个主要步骤：删除意图设置、触发条件与流转模式设置、删除通知生成、删除通知发送与转发、删除通知确认、删除操作执行、删除确认、删除存证。按需删除流程参见附录A。

6.1.2 按需删除意图设置

个人信息主体设置按需删除意图应包括但不限于：删除对象、删除时间、删除等级等。按需删除意图的输入可以通过服务商应用/网页界面进行设置。

6.1.3 按需删除触发条件与流转模式设置

按需删除触发条件与流转模式设置应遵守以下要求：

ee) 当个人信息主体无自动删除需求或法律法规无自动删除要求时，默认基于删除意图构造按需删除触发条件，并保证其不可伪造性；

ff) 按需删除触发条件应随个人信息流转配置在所有关联的个人信息源域和传播域的个人信息处理者。

6.1.4 按需删除通知生成

当满足按需删除触发条件时，按需删除通知生成应遵守以下要求：

gg) 个人信息源域的删除通知发送者根据个人信息主体需要构造按需删除通知；

hh) 按需删除通知需包含不可伪造性验证凭证。

6.1.5 按需删除通知发送与转发

当按需删除通知生成后，按需删除通知的发送与转发应遵守以下要求：

ii) 按需删除通知的发送范围要与删除对象的流转范围保持一致，可以采用逐层逐级下发的方式；

jj) 个人信息源域的删除通知发送者依据删除对象的流转路径，将按需删除通知发送给下一层关联的个人信息传播域的删除通知接收者；

kk) 收到按需删除通知后，个人信息传播域的删除通知接收者进一步依据删除对象的流转路径，将按需删除通知转发给下一层关联的个人信息传播域的删除通知接收者；

ll) 以此类推，直到删除对象关联的所有个人信息传播域的删除通知接收者均收到按需删除通知为止；

mm) 删除对象关联的个人信息源域和所有传播域的删除通知发送者将按需删除通知发送给域内个人信息删除者；

nn) 删除对象关联的所有个人信息传播域的删除通知接收者应验证按需删除通知的完整性。

6.1.6 按需删除通知确认

收到按需删除通知后，删除对象关联的所有个人信息传播域的删除通知接收者应向上一层删除通知发送者发送确认信息。

6.1.7 按需删除操作执行

删除对象关联的个人信息源域和所有传播域中的个人信息删除者收到按需删除通知后应执行按需删除操作，并遵守以下要求：