ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 40660—2021

信息安全技术
生物特征识别信息保护基本要求

Information security technology—
General requirements of biometric information protection

2021-10-11 发布　　2022-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　生物特征识别信息保护基本原则 …… 2
5　生物特征识别信息的收集 …… 2
6　生物特征识别信息的存储 …… 3
7　生物特征识别信息的使用 …… 4
8　生物特征识别信息主体的权利 …… 4
9　生物特征识别信息的委托处理、共享、转让、公开披露 …… 5
10　生物特征识别信息安全事件处置 …… 5
11　生物特征识别信息安全管理要求 …… 5
参考文献 …… 7

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、蚂蚁科技集团股份有限公司、公安部第三研究所、北京赛西科技发展有限责任公司、广州广电运通智能科技有限公司、国民认证科技(北京)有限公司、联想(北京)有限公司、格尔软件股份有限公司、北京曙光易通技术有限公司、北京眼神科技有限公司、中国信息通信研究院、公安部第一研究所、中国航空综合技术研究所、中科天地科技有限公司、深圳市腾讯计算机系统有限公司、中国科学院自动化研究所、北京市商汤科技开发有限公司、北京旷视科技有限公司、云从科技集团股份有限公司、上海依图网络科技有限公司、北京中科虹霸科技有限公司。

本文件主要起草人：刘贤刚、郝春亮、林冠辰、李俊、何延哲、郑强、于雪平、唐迪、唐健、杨晓光、宋方方、傅山、刘军、胡影、孙彦、刘新建、张默男、张堃博、成瑾、梅敬青、李军、刘亦珩、许东阳。

信息安全技术
生物特征识别信息保护基本要求

1 范围

本文件规定了各类生物特征识别信息控制者开展收集、存储、使用、委托处理共享、转让、公开披露、删除等生物特征识别信息处理活动应遵循的基本原则和安全要求。

本文件适用于规范各类生物特征识别信息控制者开展生物特征识别信息处理活动，也适用于第三方机构对生物特征识别信息处理活动进行测评。

2 规范性引用文件

下列文件中的内容通过文中的规范性引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 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

GB/T 25069、GB/T 35273—2020 界定的以及下列术语和定义适用于本文件。

3.1

生物特征识别原始信息 biometric original information

通过采集、预处理等方式获得的自然人物理、生物或行为特征的模拟或数字表示。

注：如样本、图像等。

3.2

生物特征识别比对信息 biometric comparison information

对生物特征识别原始信息进行技术处理得到的、在识别过程中用于比对的信息。

3.3

生物特征识别信息 biometric information

对自然人的物理、生物或行为特征进行技术处理得到的、能够单独或者与其他信息结合识别该自然人身份的个人信息。

注 1：生物特征识别信息包括个人面部识别特征、虹膜、指纹、基因、声纹、步态、掌纹、耳廓、眼纹等。

注 2：生物特征识别信息包含生物特征识别原始信息以及生物特征识别比对信息。

3.4

生物特征识别信息主体 biometric information subject

生物特征识别信息所标识或者关联的自然人。

3.5

生物特征识别信息控制者 biometric information controller

有能力决定生物特征识别信息处理目的、方式等的组织或个人。

3.6

撤销　revoke

阻止某个特定的生物特征识别比对信息和相应的身份相关信息通过验证。

注：一个生物特征识别信息主体被拒绝通过可能是由于其被添加到了撤销列表中。

3.7

不可逆性　irreversibility

由生物特征识别比对信息无法推断出其对应生物特征识别原始信息的特性。

3.8

不可链接性　unlinkability

两个或多个生物特征识别比对信息无法相互链接的属性。

注：具备不可链接性时，一个用户可以多次使用不同的程序、资源和服务，而其他人不能通过生物特征识别比对信息将这些使用关联在一起。

4　生物特征识别信息保护基本原则

对生物特征识别信息保护的基本原则如下。

a）　应满足 GB/T 35273—2020 中对个人信息控制者的所有要求。

b）　应遵循 GB/T 35273—2020 第 4 章中的个人信息安全基本原则，并应遵循以下原则：

1）　自主选择——在开展身份识别相关活动的场景，保证个人有使用或不使用生物特征识别信息的选择权，确保个人在自愿的情况下、通过直接方式提供生物特征识别信息，并确保个人对其生物特征识别信息持续的控制权；

2）　多样更新——使用具备不可逆、不可链接、多样化、可更新等特性的生物特征识别比对信息；

3）　充分知情——保证生物特征识别信息主体对其生物特征识别信息处理情况和安全事件的知情权。

5　生物特征识别信息的收集

对生物特征识别信息控制者的要求如下。

a）　除法律法规规定场景、保护公共利益和个人重大利益场景外，不应限定收集生物特征识别信息作为唯一实现业务目标的方式。

b）　收集生物特征识别信息前，应向生物特征识别信息主体告知以下信息，并征得生物特征识别信息主体的明示同意：

1）　收集、使用生物特征识别信息的目的、方式和范围，以及授权存储时间等；

2）　收集的生物特征识别信息处理方式的描述；

3）　生物特征识别信息控制者的联系信息，包括组织机构信息、联系方式等；

4）　生物特征识别信息主体实现查看、修改、撤回其授权同意的方式。

c）　应避免收集不属于该生物特征识别信息主体的生物特征识别信息，包括生物特征识别原始信息。

d）　应避免采用间接方式从非生物特征识别信息主体处获取其信息。

e）　生物特征识别信息主体无法完成信息收集时，应告知后续可用替代处理流程。

f）　根据国家相关法律法规等规定收集生物特征识别信息时，应将相关要求以及收集的生物特征识别信息类型告知生物特征识别信息主体。

g） 应对呈现干扰攻击风险进行充分考虑，考虑因素包括但不限于物理、虚拟等不同攻击形式，纸质、塑料等不同攻击材质，呈现角度、光线条件等不同攻击环境等。

6 生物特征识别信息的存储

对生物特征识别信息控制者的要求如下。

a） 应将生物特征识别信息与生物特征识别信息主体的身份相关信息采用技术隔离手段存储。

注 1：隔离方式包括逻辑隔离、物理隔离等。

b） 存储生物特征识别信息时，应确保其具备不可逆性。

c） 原则上不应直接存储生物特征识别原始信息，可采取的措施包括但不限于：

1） 仅存储生物特征识别信息的摘要信息；

2） 在采集终端中直接使用生物特征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、认证等功能后删除生物特征识别原始信息。

注 2：摘要信息通常具有不可逆性。

注 3：生物特征识别信息控制者履行法律法规规定的义务相关的情形除外。

d） 应使用多样化过程以支持生成可更新、可撤销的生物特征识别比对信息：

1） 多样化过程产生的生物特征识别比对信息应具备不可逆性；

2） 通过多样化过程产生的同一生物特征识别信息主体的各个生物特征识别比对信息应具有不可链接性。

注 4：多样化过程是指将一个生物特征识别信息主体的单个或多个生物特征识别原始信息变换成多个独立的生物特征识别比对信息，用于生物特征识别比对信息的更新或为不同的应用程序分别提供独立的生物特征识别比对信息。

e） 存储生物特征识别比对信息时，应充分考虑数据泄露风险、进行安全处理，可使用的机制包括但不限于：

1） 通过在个人令牌或卡上存储生物特征识别比对信息，通过逻辑、物理方式进行安全保护；

2） 使用仅生物特征识别信息控制者或生物特征识别信息主体知道的密钥执行加密操作；

3） 尽可能减少存储的生物特征识别比对信息；

4） 使用不可直接关联到生物特征识别信息主体的标识符。

f） 应保持生物特征识别比对信息在应用程序或数据库间的不可链接性，以防止生物特征识别比对信息可能被用于链接同一数据库中不同应用程序或不同数据库中的同一信息主体；不可链接性可通过以下机制的组合获得：

1） 在应用程序之间使用不同的密钥或机制对生物特征比对信息进行加密，阻止对生物特征识别信息主体的链接，原则上不同密钥应交不同人员保管；

2） 在应用程序之间使用以下方式或其组合：采用不同的生物特征识别模式、采用不兼容的特征提取算法、采用不兼容的生物特征识别数据交换格式。

g） 生物特征识别信息的复制信息，如备份信息、归档信息等，存储时应具备与被复制信息相同的保护措施。

h） 应只存储满足生物特征识别信息主体授权同意的目的所需最少的生物特征识别信息。

i） 应只在生物特征识别信息主体授权的存储时间内存储生物特征识别信息，超出存储期限后，应及时对生物特征识别信息进行删除或匿名化处理。

7 生物特征识别信息的使用

对生物特征识别信息控制者的要求如下。

a) 使用生物特征识别信息进行算法精度优化等，应彻底去除与生物特征识别信息主体的身份关联，充分评估安全风险，并在使用目标完成后及时删除相关信息。

b) 应使用可更新、可撤销、具有不可逆性的生物特征识别比对信息进行身份识别。

c) 不应基于生物特征识别信息自身生成用户画像和统计分析，包括但不限于：

1) 不应基于生物特征识别信息自身描述有关民族、种族、宗教、残疾、性取向、暴力倾向等信息；

2) 不应基于生物特征识别信息自身进行统计分析；确需统计分析时，应事先进行个人信息安全影响评估，仅使用经匿名化后的数据。

d) 不应基于生物特征识别信息自身进行个性化推荐，包括但不限于：

1) 不应基于个人基因、面部识别特征、指纹、声纹、耳廓、步态等的特点发送商业性信息；

示例：不应基于个人基因、面部识别特征、指纹、声纹、耳廓、步态的特征或变化推荐美容、医疗等服务。

2) 不应基于个人面部识别特征、声纹、步态等分析个人行为习惯、意见观点等进行信息推送。

e) 不应使用生物特征识别比对信息作为汇聚融合的直接关联点。

f) 应对生物特征识别信息的复制、下载等重要操作进行严格控制，应仅在实现已获授权同意目的所必须的情况下进行，应明确特定人员执行、保证操作过程安全、及时收回执行人员的操作权限。

8 生物特征识别信息主体的权利

对生物特征识别信息控制者的要求如下。

a) 应向生物特征识别信息主体提供查询下列信息的方法：

1) 该生物特征识别信息主体的生物特征识别信息的类型；

2) 生物特征识别信息授权同意情况，包括但不限于获得授权同意的方式与日期，已获授权同意的收集使用目的、授权存储时间等；

3) 生物特征识别信息处理情况；

4) 生物特征识别信息安全事件，如被篡改、泄露等。

b) 应对生物特征识别信息主体的以下请求做出及时响应：

1) 修改、撤回其生物特征识别信息的授权；

2) 更新生物特征识别信息。

c) 满足以下条件之一时，应及时删除或匿名化生物特征识别信息：

1) 生物特征识别信息授权存储期限已过；

2) 生物特征识别信息主体撤回对生物特征识别信息的授权；

3) 生物特征识别信息经生物特征识别信息主体授权的使用目的已经实现或确定为不必要。

d) 应根据生物特征识别信息的授权存储期限等信息，建立待删除或匿名化的生物特征识别信息清单。

e) 应明确对生物特征识别信息进行删除及匿名化处理的程序和保障措施，确保完整、安全地处理生物特征识别信息。

9 生物特征识别信息的委托处理、共享、转让、公开披露

对生物特征识别信息控制者的要求如下。

a) 生物特征识别信息原则上不应共享、转让。

b) 不应公开披露生物特征识别信息。

c) 委托第三方处理生物特征识别信息时，应预先向生物特征识别信息主体告知以下信息：

1) 第三方相关信息；

2) 所涉生物特征识别信息的类型和数量；

3) 委托处理目的。

d) 委托第三方处理生物特征识别信息，以及嵌入第三方工具处理生物特征识别信息时，应优先选择具备相应资质或能力的机构。

10 生物特征识别信息安全事件处置

对生物特征识别信息控制者的要求如下。

a) 生物特征识别信息安全事件发生时，应及时评估事件影响，应及时撤销受安全事件影响的生物特征识别比对信息，防止攻击者未经授权访问；宜及时更新受安全事件影响的生物特征识别比对信息。

b) 当有证据明确表明正在使用的生物特征识别比对信息存在风险时，如生物特征识别信息主体主动表示其生物特征识别比对信息存在泄漏风险，应及时撤销存在风险的生物特征识别比对信息，并为生物特征识别信息主体关联新的生物特征识别比对信息。

c) 因安全事件更新生物特征识别比对信息时，应进行安全评估，如存在更新生物特征识别比对信息后亦不能消除安全威胁的情况，应在撤销生物特征识别比对信息的前提下，及时使用其他的身份识别方式。

11 生物特征识别信息安全管理要求

对生物特征识别信息控制者的管理要求如下。

a) 在提供多种可供选择的身份识别方式时，不宜将使用生物特征识别信息的方式作为初始设置的默认选项。

b) 应持续开展安全风险相关的评估，及时采取措施降低处理风险，充分保障生物特征识别主体的权利，包括：

1) 在业务活动计划收集生物特征识别信息前，应评估使用生物特征识别信息的必要性，以及是否具备相应的安全能力和安全控制措施；

2) 在收集生物特征识别信息前，应进行个人信息安全影响评估，确保处理生物特征识别信息过程风险可控；

3) 在执行变更生物特征识别信息处理目的或范围、委托第三方处理、共享或转让等行为前，应进行个人信息安全影响评估，确保不引入新的安全风险；

4) 有共享、转让生物特征识别信息情况的，应定期对共享、转让生物特征识别信息的必要性进行评估；

5) 宜定期(如每年度)对现有生物特征识别信息处理情况进行重新评估，确保现有安全措施满足当下安全需求。

c) 应建立、维护生物特征识别信息处理活动记录，记录的内容宜包括：
   1) 所控制的生物特征识别信息类型、来源；
   2) 生物特征识别信息授权情况；
   3) 生物特征识别信息处理情况。
d) 应针对不同类型、不同处理阶段生物特征识别信息制定保护计划，并宜向相关生物特征识别信息主体公开保护计划。
e) 应对生物特征识别原始信息的传输进行有效控制，宜采取水印等技术手段保障生物特征识别原始信息可溯源。
f) 对因终止生物特征识别相关活动删除或匿名化生物特征识别信息的情况，应对删除或匿名化效果进行评估。
g) 基于生物特征识别信息的身份识别相关算法，以及开展生物特征识别相关活动时收集的生物特征识别信息原则上不应出境、出口；如有特殊原因需出境、出口，应经相关主管部门审批。
h) 本文件凡涉及密码算法的相关内容，按国家有关法规实施；凡涉及采用密码技术解决保密性、完整性、真实性、不可否认性需求的应遵循密码相关国家标准和行业标准。

参 考 文 献

[1] ISO/IEC 24745:2011 Information technology—Security techniques—Biometric information protection

[2] ISO/IEC 30107-1:2016 Information technology—Biometric presentation attack detection—Part 1:Framework