ICS 35.020
CCS L 70

DB21

辽 宁 省 地 方 标 准

DB21/T XXXX—XXXX

面部识别通用规则

General rules for facial recognition

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省市场监督管理局　　发 布

目　　次

前言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　概述 1
4.1　综述 1
4.2　处理 2
4.3　应用场景 2
4.4　安全性 2
5　知情同意 2
5.1　要求 2
5.2　告知信息 3
5.3　例外 3
6　权利主张 3
6.1　要求 3
6.2　权利保障 3
7　个人信息管理者 3
8　管理机制 4
8.1　责任主体 4
8.2　管理 4
8.3　管理制度 4
8.4　人员管理 4
8.5　文档管理 5
9　数据库管理 5
9.1　存储方式 5
9.2　要求 5
9.3　安全机制 5
10　采集过程 5
10.1　要求 5
10.2　直接采集 5
10.3　间接采集 5
10.4　被动采集 6
11　处理过程 6
11.1　要求 6
11.2　过程控制 6

11.3 后处理 7
12 安全管理 8
12.1 风险管理 8
12.2 安全机制 8
13 过程管理 8
附录 A（资料性） 基于个人信息主体画像的面部特征信息开发示例 9

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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：大连软信咨询服务有限公司、大连软件行业协会、大连交通大学、大连华信计算机技术股份有限公司、大连奥远电子股份有限公司、辽宁省信息中心、辽宁省社会保险事业服务中心、大连理工现代工程检测有限公司、大连市计算机学会。

本文件主要起草人：郎庆斌、尹宏、刘宏、胡剑锋、于青、杨万清、杨莉、唐文伟、才昊、明晓浙、邓连峰、于昕、金成明、丁宗安、秦健、王鑫、司丹、孙毅、王小庚。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件归口单位通讯地址：沈阳市北陵大街45-2号，联系电话：024-86913384

本文件起草单位通讯地址：大连市高新园区火炬路32号创业大厦A座5层，联系电话：0411-83655207

面部识别通用规则

1 范围

本文件规定了面部特征信息识别的知情同意、权利主张、个人信息管理者、管理机制、数据库管理、采集过程、处理过程、安全管理和过程管理等相关要求。

本文件适用于指导面部特征信息识别应用场景的应用、管理、过程等。

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。

DB21/T 1628.1-2016 信息安全 个人信息保护规范

DB21/T 1628.2-2018 信息安全 个人信息安全管理体系 第2部分：实施指南

DB21/T 1628.4 信息安全 个人信息安全管理体系 第4部分：个人信息管理文档管理指南

DB21/T 1628.5 信息安全 第5部分：个人信息安全风险管理指南

DB21/T 1628.6 信息安全 个人信息安全管理体系 第6部分：安全技术实施指南

DB21/T 1628.7 信息安全 个人信息安全管理体系 第7部分：内审实施指南

DB21/T 1628.8 信息安全 个人信息安全管理体系 第8部分：过程管理指南

3 术语和定义

DB21/T 1628界定的以及下列术语和定义适用于本文件。

3.1

面部特征 facial features

自然人面部特定部位或整体的特征信息。

3.2

面部识别 facial recognition

基于自然人面部特征信息识别个人信息主体的一种生物识别技术。

3.3

个人信息主体画像 personal information subject profile

勾画个人信息主体基本特征，描摹个人信息主体基本形象。

4 概述

4.1 综述

自然人面部特征信息是敏感的个人信息，但在社会生活中，随着科技进步、社会发展，与身份证号码、手机号码、银行卡号等一样，成为社会生活中经常用到的个人信息，亦具有了个人信息处理过程的

敏感性。与身份证号码、手机号码、银行卡号等不同，自然人的面部特征信息无法更改，一旦泄露，个人信息主体权益可能永久灭失。

4.2 处理

面部特征信息识别是基于自然人面部特征信息识别个人信息主体的生物识别技术，技术处理活动主要包括：

a) 图像采集：借助相关设备采集含自然人面部特征信息的图像或视频流；
b) 图像检测：含自然人面部特征信息图像或视频流的精度、准确率、可用性等检测；
c) 图像存储：含自然人面部特征信息或视频信息等的数据库存储系统；
d) 图像处理：包括基于图像检测的图像预处理、图像特征提取等图像的处理过程；
e) 图像识别和匹配：分析比较自然人面部特征信息的个人信息主体识别，或基于已知数据库存储的自然人面部特征模板与采集的自然人面部图像特征信息比较、匹配；
f) 图像传输：含自然人面部特征信息、图像信息、视频信息等的传送、交换过程等。

4.3 应用场景

采集自然人面部特征信息的应用场景主要包括：

a) 在社会活动、生活实践中获得各种公共服务时直接或间接采集，如公安、金融、机场、地铁，及办公、教育、医疗、社区管理等；
b) 基于公共利益或公共安全被动采集含自然人面部特征信息的图像或视频流，如交通枢纽监控、道路抓拍、安防监控、门禁系统等；
c) 基于商业应用的被动采集，如超市、商业网点等；
d) 个人信息管理者内部应用的直接采集，如考勤等；
e) 其它应用场景等。

4.4 安全性

自然人面部特征信息，与基因、虹膜、指纹及其它自然人生物特征信息，是敏感的个人信息。随着社会发展、科技进步进入社会活动、生活实践中，面部特征信息的敏感性过渡为个人信息处理过程的敏感性，但是，面部特征信息的敏感特征没有改变，未知的安全风险增大且难以预测，自然人面部特征信息存在永久灭失的风险。

对自然人面部特征信息的管理，应符合DB21/T 1628系列标准要求。

5 知情同意

5.1 要求

依据DB21/T1628.1，各种应用场景采集含自然人面部特征的信息，应以浅显易懂且可理解的方式明确告知个人信息主体：

a) 直接采集自然人面部特征信息时，应以明确的方式告知个人信息主体并征得个人信息主体明确同意；
b) 间接或被动方式采集自然人面部特征信息时，应借助各种媒介、媒体发布公示、公告等各种方式明确告知个人信息主体并宜以各种方式征得个人信息主体明确同意。

5.2 告知信息

告知个人信息主体的信息应包括：

a) 面部特征信息采集的目的、用途；
b) 个人信息主体的权利；
c) 个人信息管理者的责任；
d) 面部特征信息采集的方式方法；
e) 面部特征信息的存储、处理方式；
f) 安全承诺；
g) 面部特征信息处理之后的处理方式；
h) 争议仲裁方式等。

5.3 例外

基于以下情况，个人信息主体应知悉：

a) 基于公共卫生、公共安全、公众利益的应用场景，可不需征得个人信息主体明确同意，应以公示、公告等形式公开告知。告知内容参照 5.2；
b) 不以识别个人信息主体为目的的生物识别技术（如自动驾驶技术），应参照 5.2 告知相关自然人，并明确说明应用场景、应用场景与自然人的关联关系、与自然人相关信息的处理方式等。

6 权利主张

6.1 要求

应用面部特征信息识别技术，应依据DB21/T1628.1-2016第5章，明确申明个人信息主体权利：

a) 应直接告知个人信息主体应具有的权利；
b) 应以公示、公告等书面形式公开告知个人信息主体权利。

6.2 权利保障

个人信息主体对面部特征信息识别技术应用提出质疑或反对时：

a) 应暂停面部特征信息识别技术应用；
b) 应听取个人信息主体的意见，与个人信息主体沟通、协商；
c) 如个人信息主体意见正当、合理、合法，应做出适当安排，满足个人信息主体的诉求；
d) 如个人信息主体意见有误，应予解释、说明；
e) 5.3 的例外应保障个人信息主体的权利。

7 个人信息管理者

采集、存储、管理、处理、使用自然人面部特征信息的个人信息管理者，应遵循DB21/T 1628.1 、DB21/T 1628.2确立的规则，并在采集、存储、管理、处理、使用自然人面部特征信息时确认第5章、第6章规则。

8 管理机制

8.1 责任主体

8.1.1 最高管理者

依据DB21/T 1628.1、DB21/T 1628.2，个人信息管理者的最高管理者应重视、明确认知自然人面部特征信息的安全风险，指定适宜的管理者代表，组建或明确相应的责任主体。

8.1.2 管理者代表

依据DB21/T 1628.1、DB21/T 1628.2，管理者代表应组建或指定相应的责任主体，明确职能、职责、资源、能力等，保证面部特征信息管理的有效性、可靠性、安全性。

8.2 管理

8.2.1 要求

应基于DB21/T 1628.1、DB21/T 1628.2，确立面部特征信息管理的基本规则。

8.2.2 策略

应依据DB21/T 1628.1-2016第8章、DB21/T 1628.2-2018中10.2节，制定面部特征信息管理的基本策略。

8.2.3 计划

应基于DB21/T 1628.1、DB21/T 1628.2，编制适于面部特征信息采集、存储、管理、处理、使用等的管理计划。

8.2.4 体系

为保证面部特征信息管理的有序、规范、安全，宜依据DB21/T 1628.1、DB21/T 1628.2建立相应的管理体系。

8.3 管理制度

应参照DB21/T 1628.1、DB21/T 1628.2，依据面部特征信息采集、存储、管理、处理、使用及后处理的处理方法等全流程的特征，制定相应的管理制度。

8.4 人员管理

8.4.1 管理设计

应参照DB21/T 1628.1、DB21/T 1628.2，依据面部特征信息采集、存储、管理、处理、使用及后处理的处理方法等全流程的安全特征、管理特征，设计并建立与面部特征信息管理相关人员、个人信息管理相关人员、及其他可能与之相关人员的管理策略和机制。

8.4.2 培训教育

应依据DB21/T 1628.1、DB21/T 1628.2，建立与面部特征信息管理相关人员、个人信息管理相关人员、及其他可能与之相关人员的、适应面部特征信息管理的相关培训教育计划、制度、实施方案等。

8.5 文档管理

应参照DB21/T 1628.1、DB21/T 1628.2、DB21/T 1628.4，建立并完善面部特征信息采集、存储、管理、处理、使用及处理后的处理方法等全流程的相关文档管理机制，保证面部特征信息管理的可检索、可追溯。

9 数据库管理

9.1 存储方式

自然人面部特征信息数据库，可包括2种存储方式：

a）本地存储：个人信息管理者管理、控制的数据存储系统；

b）云存储：基于网络的在线存储模式。

9.2 要求

应参照DB21/T 1628.1、DB21/T 1628.2、DB21/T1628.3，基于自然人面部特征信息存储方式、安全特征，建立适于面部特征信息数据库管理的相关管理机制。

9.3 安全机制

应参照DB21/T 1628.1、DB21/T 1628.2、DB21/T1628.3及相关标准，建立面部特征信息数据库安全机制：

a) 本地存储：应参照 DB21/T 1628.1、DB21/T 1628.2、DB21/T1628.3，建立安全机制；

b) 云存储：应建立基于云端存储的面部特征信息数据库的安全模型，根据云存储的安全特征，建立相应的安全机制。

10 采集过程

10.1 要求

应参照DB21/T 1628.1-2016 11.1、DB21/T 1628.2-2018第13章和本文件的规则，根据不同应用场景的特征，规范自然人面部特征信息采集的约束规则，并应保证：

a) 自然人面部特征信息采集应限于应用目的，不应超目的采集；

b) 自然人面部特征信息应限于应用目的适度采集，不应过度采集；

c) 自然人面部特征信息采集应合法、合规且必要。

10.2 直接采集

在各种应用场景中直接采集自然人面部特征信息，应严格遵循DB21/T 1628.1、DB21/T 1628.2和本文件确立的规则，保证自然人面部特征信息采集的规范、合理、安全。

10.3 间接采集

在各种应用场景采用非直接方式采集自然人面部特征信息，如视频（图像）分享、人工智能应用、基于公共安全或公共卫生或公众利益的应用、个人信息主体画像分享等 ，应严格遵循DB21/T 1628.1、DB21/T 1628.2和本文件确立的规则，保障个人信息主体权益，保证自然人面部特征信息可控、安全。

10.4 被动采集

在各种应用场景中，存在个人信息主体不知情或不能控制情况下被动采集自然人面部特征信息，如商业应用、公共安全等，应严格遵循DB21/T 1628.1、DB21/T 1628.2和本文件确立的规则，保障个人信息主体的权利、权益。

11 处理过程

11.1 要求

应参照DB21/T 1628.1-2016第11章、DB21/T 1628.2-2018第14章和本文件的规则，根据不同使用需求的特征，规范自然人面部特征信息处理的约束规则。

11.2 过程控制

11.2.1 提供

个人信息管理者向第三方提供自然人面部特征信息时，应遵循DB21/T 1628.1-2016中11.3.1的规则，并应保证：

a) 因公共管理、公共卫生、公共利益、公共安全等确有必要；
b) 自然人面部特征信息来源应是合法、精确、有效的直接采集；
c) 个人信息主体应明确知情同意；
d) 个人信息主体的权益。

11.2.2 委托

个人信息管理者委托第三方采集自然人面部特征信息，或委托第三方处理合法拥有的自然人面部特征信息时，应遵循DB21/T 1628.1-2016中11.3.2的规则，并应参照12.2.1提供保证。

11.2.3 个人信息主体画像

11.2.3.1 形式

基于个人信息主体画像处理的基本形式，主要包括：

a) 基于自然人照片识别个人信息主体、提取面部特征信息或处理与个人信息主体相关的业务；
b) 基于自然人的基本描摹，采集个人信息主体面部特征信息，处理与个人信息主体相关的业务；
c) 基于视频、摄像、录像等技术提取个人信息主体面部特征信息，处理与个人信息主体相关业务；
d) 其它形式等。

11.2.3.2 要求

基于个人信息主体画像处理，应参照DB21/T 1628.1-2016第11章、DB21/T 1628.2-2018第14章和本文件的规则，根据不同的个人信息主体画像应用场景和应用特征，规范与个人信息、个人信息主体相关处理的约束规则：

a) 应保证个人信息主体画像识别的真实性、准确性；
b) 应保证基于个人信息主体画像处理的公正性、公平性；
c) 应保证个人信息主体画像相关个人信息主体的权利、权益；
d) 应参照 12.2.1 提供保证等。

11.2.4 开发

11.2.4.1 描述

开发自然人面部特征信息，是基于个人信息主体画像的深度剖析，通过分析、整合、整理、挖掘、加工等，识别自然人面部特征信息的价值属性、关联的特征信息、丰富内涵等。参看附录A。

11.2.4.2 可控性

开发自然人面部特征信息的，应遵循DB21/T 1628.1-2016中11.3.3.1、DB21/T 1628.2-2018中14.7的规则，保证个人信息主体对面部特征信息的可控性：

a) 应保证 DB21/T 1628.1-2016 第 4 章确立的个人信息主体的权利；
b) 开发自然人面部特征信息，应明确开发目的；
c) 开发自然人面部特征信息，应限定在个人信息主体明确同意的目的范围内；
d) 开发自然人面部特征信息，应依据 DB21/T 1628 建立严格的管理机制、策略；
e) 开发自然人面部特征信息，应采取严格的安全措施等。

11.2.4.3 要求

基于个人信息主体画像提取自然人面部特征信息并进行挖掘、加工等开发活动，应：

a) 保证个人信息主体画像来源的合法性、准确性；
b) 保证提取个人信息主体画像的自然人面部特征信息开发的合法性、合理性；
c) 参照 11.2.4.2 的要求。

11.2.4.4 交易

应参照DB21/T 1628.1-2016第16章的规则，禁止基于自然人面部特征信息的交易行为。如确有需要，如公共管理、公共卫生等，可存在交换行为，但应采取特别的安全防护措施，并参照11.2.4.2的规则。

11.3 后处理

11.3.1 要求

应遵循DB21/T 1628.1-2016中11.5、DB21/T 1628.2-2018中14.8的规则，确定自然人面部特征信息处理、使用后的处理方式。

11.3.2 存储

自然人面部特征信息处理、使用后需要保存，应遵循DB21/T1628.3的规则和本文件，建立独立的面部特征信息数据库，规范和持续完善管理机制和策略，保证面部特征信息质量。

注：面部特征信息数据库应是独立的，但应依据DB21/T 1628.1、DB21/T 1628.2、DB21/T1628.3，与个人信息数据库形成统一的管理机制。

11.3.3 销毁

自然人面部特征信息处理、使用后，如不存在继续保存、使用的必要性，不需继续保存、使用，应彻底销毁与自然人面部特征信息相关的文档、介质等及其记录的自然人面部特征信息。

12 安全管理

12.1 风险管理

应参照DB21/T 1628.1、 DB21/T 1628.5的规则，根据不同的应用场景，对自然人面部特征信息采集、处理、使用及与之相关的资源实施风险管理，识别可能存在的风险源，采取相应的安全措施。

12.2 安全机制

应遵循信息安全相关国家法规、标准和DB21/T 1628.1、 DB21/T 1628.6，基于风险管理，采用相应的安全技术，建立相应的安全机制、安全管理体系，保障面部特征信息采集、处理、使用和面部特征信息数据库的安全、可靠。

13 过程管理

应参照DB21/T 1628.1、 DB21/T 1628.2、 DB21/T 1628.7、 DB21/T 1628.8，建立自然人面部特征信息采集、处理、使用、存储及处理、使用后处理全过程的管理机制，保证自然人面部特征信息采集、处理、使用、存储及处理、使用后处理全过程的安全、可控、可信。

附　录　A
（资料性）
基于个人信息主体画像的面部特征信息开发示例

与个人信息的二次开发类同，基于个人信息主体画像的面部特征信息开发，如：
个人信息主体的人格要素：年龄、性别、地域、教育程度、职业等；
个人信息主体的行为特征：旅游、房产、体育、购物、交友等；
个人信息主体的消费特征：购物兴趣、消费能力等；