ICS 35.040
L80

GB/T 35273 2020
GB/T 35273-2017

信息安全技术　个人信息安全规范

Information security technology　Personal information security specification

2020-03-06　　2020-10-01

目　　次

前 言

GB/T 1.1 2009

GB/T 35273-2017 GB/T 35273-2017

“ ” 5.3

“ ” 5.6 2017 5.4

“ ” 7.4

“ ” 7.5

“ ” 7.6

“ ” 8.5 2017 7.8

“ ” 9.7

“ ” 11.1 2017 10.1

“ ” 11.2

“ ” 11.3

“ ” C 2017 C

SAC/TC260

引　　言

信息安全技术　个人信息安全规范

1　范围

2　规范性引用文件

GB/T 25069　2010

3　术语和定义

GB/T 25069　2010

3.1

个人信息　personal information

注 1：

注 2：　　A

注 3

3.2

个人敏感信息　personal sensitive information

注 1：

14

注 2：　　B

注 3

3.3

个人信息主体 personal information subject

3.4

个人信息控制者 personal information controller

3.5

收集 collect

3.10

删除 delete

3.11

公开披露 public disclosure

3.12

转让 transfer of control

3.13

共享 sharing

3.14

匿名化 anonymization

注

3.15

去标识化 de-identification

注：

3.16

个性化展示 personalized display

3.17

业务功能 business function

注：

4 个人信息安全基本原则

a)

b)

c)

d)

e)

f)

g)

5 个人信息的收集

5.1 收集个人信息的合法性

a)

b)

c)

5.2 收集个人信息的最小必要

a)

b)

c)

5.3 多项业务功能的自主选择

a)

b)

c)

5)

6)

7)

8)

b)
c)

d)

C

e)

f) a

注1： “ ”

注2： D

注3：

5.6 征得授权同意的例外

a)
b)
c)
d)
e)

f)
g)

注：

h)

i)

j)

k)

6 个人信息的存储

6.1 个人信息存储时间最小化

a)

b)

6.2 去标识化处理

6.3 个人敏感信息的传输和存储

a)

注：

b)

c)

1)

2)

3)

注1：

注2：

6.4 个人信息控制者停止运营

a)

b)

c)

7 个人信息的使用

7.1 个人信息访问控制措施

a)

b)

c)
d)

注： 11.1
e)

7.2 个人信息的展示限制

7.3 个人信息使用的目的限制

a)

注：

b)

注：

7.4 用户画像的使用限制

a)
    1)
    2)
b)
    1)
    2)

c)

7.5 个性化展示的使用

a)

注： “ ”

b)

注：

c)
1)
2)

d)

7.6 基于不同业务目的所收集个人信息的汇聚融合

a) 7.3
b)

7.7 信息系统自动决策机制的使用

a)

b)

c)

8 个人信息主体的权利

8.1 个人信息查询

a)

b)

c)

注

8.2 个人信息更正

8.3 个人信息删除

a)

1)

2)

b)

c)

注 2：

e)

f)

8.6 个人信息主体获取个人信息副本

a)
b)

8.7 响应个人信息主体的请求

a) 8.1~8.6

b)

c)

d)

e) 8.1~8.6
1)
2)
3)
4)
5)

6)

7)

8)
f)

8.8 投诉管理

9 个人信息的委托处理、共享、转让、公开披露

9.1 委托处理

a)
5.6
b)
11.5
c)
1)

2)
3) 8.1~8.6
4)

5)
d)
1)
2)
e)
f)

9.2 个人信息共享、转让

a)

b)

c) b

d)

e)

f)

g)

h)

i)

9.3 收购、兼并、重组、破产时的个人信息转让

a)
b)

c)

9.4 个人信息公开披露

a)

b)

c) b

d)

e)
f)
g)

9.5 共享、转让、公开披露个人信息时事先征得授权同意的例外

a)
b)

c)
d)
e)

f)
g)

9.6 共同个人信息控制者

a)

b)

注：

SDK API

9.7 第三方接入管理

9.1 9.6

a)

b)

c)
d)
e)

f)

g)

h)

1)
2)

9.8 个人信息跨境传输

10 个人信息安全事件处置

10.1 个人信息安全事件应急处置和报告

a)
b)

c)

1)

2)
3)

4)

10.2

d)

10.2 安全事件告知

a)

b)
1)
2)
3)
4)
5)

11 组织的个人信息安全管理要求

11.1 明确责任部门与人员

a)

b)

c)

1) 200
2) 100 12 100

3) 10

d)

1)

2)
3)
4)

5)

6)
7)

8)
9)
10)

e)

11.2 个人信息安全工程

11.3 个人信息处理活动记录

a

b

c

11.4 开展个人信息安全影响评估

a)

b)

1)
2)

3)
4)

5)

6)
c)

d)

e)

f)

11.5 数据安全能力

11.6 人员管理与培训

a)

b)

c)

d)

e) ;
f)

11.7 安全审计

a)
b)
c)
d)
e)
f)

附 录 A
（资料性附录）
个人信息示例

A.1

表A.1 个人信息举例

	IP
	（ ）
	MAC IMEI/Android ID/IDFA/OpenUDID/GUID/SIM IMSI

附 录 B
（资料性附录）
个人敏感信息判定

14

B.1

表B>176*176o676*176o676*176o676*176oQ q 0. q 0.000008871 0 59

附 录 C
（资料性附录）
实现个人信息主体自主意愿的方法

C.1 概述

C.2 区分基本业务功能和扩展业务功能

a)

注1：

注2：

b)

c)

C.3 基本业务功能的告知和明示同意

a)

“ ” “ ”

注：

a)

b)

c) a

注： C.5

C.4 扩展业务功能的告知和明示同意

a)

b)

48h

c)

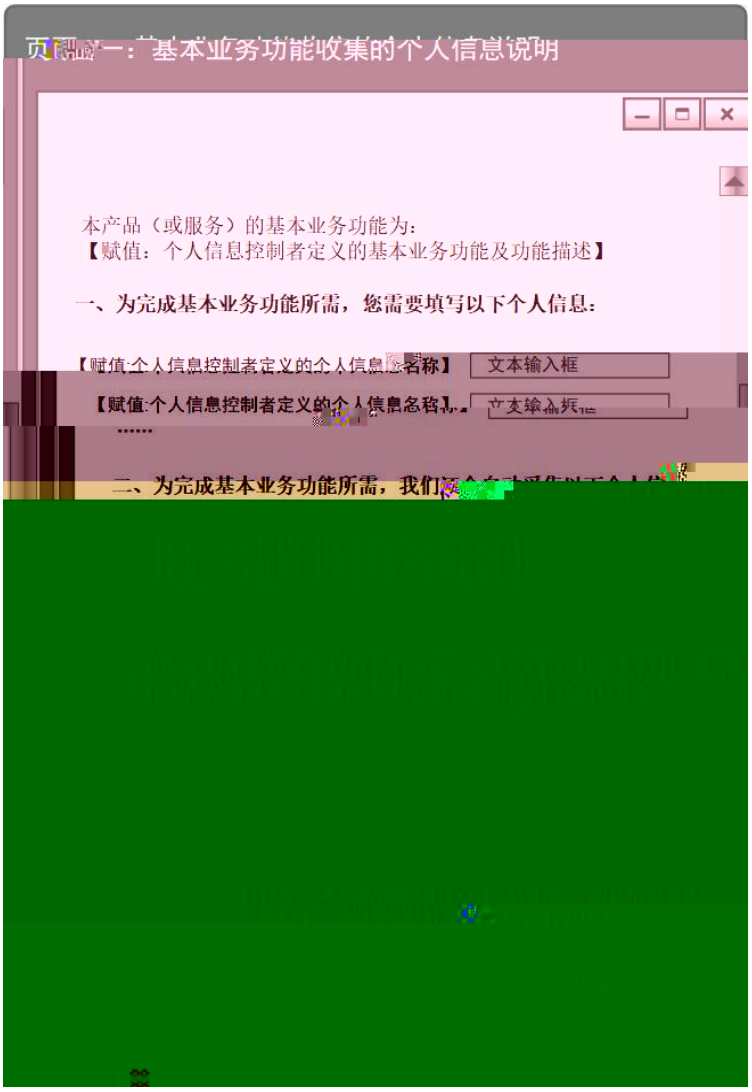
d) a

注： C.5

C.5 交互式功能界面设计

C.1

表C.1 交互式功能界面模板

功能界面模板	说明
	1 2 3 4 5 “ ”

表C.1　（续）

功能界面模板	说明
	6 7 8 9

表C.1 （续）

功能界面模板	说明
	10 11 12 13 14

表D.1 （续）

个人信息保护政策模版	编写要求
1	1
● …… XX	2
● …… XX	3
● App …… XX	4
App	5
2	
● ……	6
● …… **3**	
1	7
5 2019 12 31	
2 a) …… b) …… c) ……	
3 a) b)	
4 a) b)	

表D.1 （续）

个人信息保护政策模版	编写要求
	1
?-?-	
?-?-	
?-?-	
	2
?-?-	
	3 ”

表D.1 （续）

个人信息保护政策模版	编写要求
…… Web ?-?- 30 ?-?- “ ” Web ?-?- 30 1 2 3 4 5 …… ……	1 2 3 4 5 6

表D.1　（续）

个人信息保护政策模版	编写要求
…… …… …… 1 2 3 4 5 6 7	

表D.1 （续）

个人信息保护政策模版	编写要求
14	
/	

表D.1　（续）

个人信息保护政策模版	编写要求
1 2 3 4 5 6	
…… …… ……	1 2