ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX—XXXX

信息安全技术 个人信息安全 术语

Information security technology-Personal information security terminology

（征求意见稿）

（本草案完成时间：2023-1-10）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

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

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。

本文件由中共辽宁省委网络安全和信息化委员会办公室提出并归口。

本文件起草单位：大连软件行业协会、国家计算机网络应急技术处理协调中心辽宁分中心、大连交通大学、大连理工现代工程检测有限公司、大连软信咨询服务有限公司、大连市计算机学会。

本文件主要起草人：郎庆斌、李凯、才昊、孙鹏、尹宏、秦健、宋悦、杨莉、司丹、孙毅、曹剑、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：沈阳市和平区光荣街26号甲，联系电话：024-81680033

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

引　言

在个人信息安全实践和个人信息安全相关标准实践中，各种新鲜的术语、概念频出，衍生出的语境易于混淆，产生混乱，对个人信息安全生态产生不可逆的深刻影响。

因此，在DB21/T 1628个人信息安全标准系列十数年实践中，需要梳理、厘清、定义个人信息安全相关术语和基本概念，形成科学、规范、有效的个人信息安全相关术语体系。

信息安全技术 个人信息安全 术语

1 范围

本文件定义并描述了个人信息安全相关的术语。

本文件适用于个人信息安全相关的：

a) 与个人信息安全相关的各级各类个人信息管理者；

b) 从事个人信息安全相关活动的各类组织；

c) 各类个人信息安全相关培训、教育；

d) 评价、认证个人信息安全的相关人员、组织；

e) 研制个人信息安全相关标准的人员、组织等。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

个人 personal

基于自然规律出生，具有生物学意义和法理人格，并被赋予民事主体资格，享受民事权利并承担民事义务的自然人个体。

注1：个人泛指自然人群体中的单个个体，具有多义性。

3.2

个人信息 personal information

依附于个人，并可描述个人基本形态的信息，包括：

a) 可通过听觉、视觉、触觉等感官直接识别个人的信息，如数字、文字、图像、影像、声音等；

b) 可借助各种手段间接识别个人的信息，如与个人相关各种信息对照、参考、分析等。

注2：个人信息包括敏感的个人信息和过程敏感的个人信息：

敏感的个人信息：包括某些生理特征、健康信息、刑事纪录等不便示人的个人私密的隐私信息；

过程敏感的个人信息：包括手机号码、身份证信息、银行信息等在个人信息收集、处理、使用过程中产生的信息敏感性。

3.3

已识别个人信息主体 identified personal information subject

通过已识别个人信息主体获取其个人信息。

3.4

可识别个人信息 identifiable personal information

可通过个人信息识别个人信息主体。

3.5

个人信息质量 personal information quality

个人信息的完整性、准确性和时效性。

3.6

主体 subject

事务、信息等的所有者、支配着、控制者。

3.7

个人信息主体 personal information subject

可通过个人信息识别，享有个人信息权益，具有2.3定义的主体特征的自然人群体中的特定个人。

注3：个人信息主体具有唯一性。个人信息主体将 “个人”具象为个人信息的主体。

3.8

个人信息主体权益 personal information subject rights and interests

个人信息主体的人格权和人格利益。

注4：基于个人信息主体权益形成个人信息主体知情、控制、质疑等权利。

3.9

个人信息管理者 personal information controller

获个人信息主体授权，基于特定、明确、合法目的，获取、管理个人信息的机关、企业、事业、社会团体等组织及个人。

注5：a)个人信息处理者、个人信息控制者、个人信息消费者等应是个人信息管理者的细分;

b）这些细分角色，仅具有部分个人信息管理职能;

c）这些细分角色应具有个人信息管理者同样的责任和义务。

3.10

个人信息匿名 personal information anonymous

消除个人信息的属性特征，变异为一般性的琐碎信息，不可识别特定的个人信息主体。

注6：个人信息匿名化后仍存在复原的可能，因而，匿名化的个人信息仍然属于个人信息安全范畴。

3.11

个人信息假名 personal information pseudonym

将个人信息分解为可识别特征信息和琐碎信息,分别保存、管理。二者匹配可构成完整的个人信息，并可识别特定的个人信息主体。

4 管理过程

4.1

个人信息管理 personal information management

在个人信息生命周期内，计划、组织、协调、控制个人信息及相关资源、环境，构建管理体系等的相关活动或行为。

4.2

个人信息安全 personal information security

以安全为目的、以个人信息资源为核心，以服务管理流程为导向，构建相对稳定、安全的个人信息环境。

4.3

个人信息生命周期 personal information life cycle

当个人信息主体同意直接收集个人信息直至个人信息彻底销毁的生命历程，是个人信息管理者向个人信息主体提供服务管理的过程。

注7：个人信息生命周期可以是多重的，如间接收集应是个人信息生命周期内存在的新的生命周期。

4.4

个人信息安全管理体系 personal information security management system

个人信息管理活动或行为的结果。基于个人信息管理目标，整合目标、方针、原则、方法、过程、审核、改进等管理要素，及实现要素的方法和过程，提高个人信息管理有效性的系统。

4.5

个人信息管理机制 personal information management mechanism

个人信息管理中各种相关管理要素的内在关联、机理，并通过个人信息安全管理体系集成，保证管理目标的实现。

注8：管理机制可包括最高管理者、组织机构、管理方针（政策）、管理计划、规章制度、人员管理、文档管理……

4.6

个人信息管理方针（隐私政策）personal information management Policy（Privacy Policy）

个人信息管理者在个人信息生命周期内管理个人信息的策略、方式、方法等，以保障个人信息安全。

5 过程管理

5.1

个人信息数据库 personal information database

个人信息主体明确同意并授权，合法拥有的个人信息，按照某种方式和规则组织，形成逻辑统一的个人信息集合体。包括：

a) 可以通过自动处理方式处理、使用的、特定的个人信息集合体；

b) 可以采用非自动处理方式处理、使用的、特定的个人信息集合体；

c) 前述 2 种混合形式；

除前3项外，法律规定的可检索特定个人信息的集合体。

注9：个人信息数据库的存储介质可包括磁介质、电子、网络媒介；纸介质、声音、照片等。

5.2

个人信息收集 personal information collect

基于特定、明确、合法的目的采集并获取个人信息的行为。

注10：收集是处理活动的内容，但是处理的源头，应提炼并规范。

注11：收集可分为：

直接收集：直接从个人信息主体收集个人信息；

间接收集：采用各种合法方式非直接地从个人信息主体收集自然人的个人信息；

被动收集：间接收集的特例，但个人信息主体不知情或不能控制，并且事前、事后均未通知个人信息主体，未获得个人信息主体的明确同意。

5.3

个人信息处理 personal information process

处置个人信息的过程，如收集、加工、编辑、存储、检索、交换、传输等及其它使用行为或活动。处理活动或行为可分为自动处理和非自动处理。

5.3.1

自动处理 automatic processing

利用计算机及其相关和配套设备、信息网络系统、信息资源系统等，按照一定的应用目的和规则，收集、加工、编辑、存储、检索、交换、传输等个人信息相关处置活动或行为。

5.3.2

非自动处理 non-automatic processing

除自动处理外的其它个人信息处置行为或活动。

5.4

个人信息利用 personal information utilize

因某种利益使用个人信息或因某种利益交付第三方使用个人信息的行为。

5.5

个人信息提供 personal information provide

合法拥有个人信息的个人信息管理者向其它个人信息管理者合法提交个人信息使用的处理过程。

5.6

个人信息委托 personal information authorise

个人信息管理者之间依法托付个人信息相关处理、使用业务。

注12：个人信息跨境传输应视为一种个人信息委托业务。

5.7

个人信息主体画像 personal information subject profiling

根据已获得的个人信息主体的相关表征信息，勾勒、描摹个人信息主体的基本特征。

5.8

个人信息开发 personal information develop

基于已知个人信息的深度挖掘、分析、整合、加工，以获取、分析、评价个人信息主体的个人偏好、行为模式、社会经历等。

5.9

个人信息主体同意 personal information subject agreement

个人信息管理活动或行为与个人信息主体意愿一致，个人信息主体明确表示赞成。表达形式包括：

a) 个人信息主体以书面形式同意；

b) 个人信息主体以可鉴证的、有规范记录的、满足书面形式要求的非书面形式同意。

注13：下述情况视为个人信息主体同意：

1）由监护人代表未成年的或无法做出正确判断的成年个人信息主体表达的意愿；

2）个人信息管理者与个人信息主体签订合同中确认了相关个人信息处理的规定，个人信息主体同意履行合同。

5.10

个人信息共享 personal information sharing

在提供个人信息等处理活动或行为中，提供者与被提供者共同享有个人信息的使用权。

注14：个人信息共享不应等同于提供者和被提供者均具有控制权，应具有同等的管理职能，保证个人信息主体的权益。

5.11

个人信息转移 personal information transfer

个人信息提供的一种形式。

5.12

个人信息安全管理体系内审 personal information security management system internal audit

个人信息管理者对个人信息安全管理体系的法律、标准的符合性、有效性及个人信息安全目标是否达成的内部独立分析、判断和评价。

参 考 文 献

[1] GBT 35273-2020 信息安全技术 个人信息安全规范
[2] GB/Z 28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
[3] T/SIA001-2017 企业个人信息安全管理规范
[4] DB21/T 1628.1 信息安全 个人信息保护规范