

ICS 35.030
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 45652-2025

**Cybersecurity technology - Security specification for generative
artificial intelligence pre-training and fine-tuning data**

网络安全技术 生成式人工智能预训练和优化训练数据安全规范

Issued on: April 25, 2025

Implemented on: November 1, 2025

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

Preface	III
Introduction	IV
1 Scope	1
2 Normative references	1
3 Terms and Definitions	1
4 General safety requirements	2
5 Security requirements for pre-training data processing activities	3
5.1 Data Collection	3
5.2 Data Preprocessing	3
5.3 Data Usage	4
6 Optimizing security requirements for training data processing activities	4
6.1 Data Collection	4
6.2 Data Preprocessing	5
6.3 Data Usage	5
7 Evaluation Methods	5
7.1 General safety assessment method	5
7.2 Evaluation Methods for Pre-training Data Processing Activities	7
7.2.1 Data Collection	7
7.2.2 Data Preprocessing	8
7.2.3 Data usage	10
7.3 Optimizing the evaluation method of training data processing activities	10
7.3.1 Data Collection	10
7.3.2 Data Preprocessing	11
7.3.3 Data Usage	12
Reference	14

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

Please note that some of the contents of this document may involve patents. The issuing

organization of this document does not assume the responsibility for identifying patents.

This document was proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260).

This document was drafted by: Beijing Zhongguancun Laboratory, National Computer Network Emergency Response Technical Processing Coordination Center, China Electronics Technology Standards Institute of Chemistry, Peking University, Beijing Topsec Network Security Technology Co., Ltd., Beijing Kuaishou Technology Co., Ltd., Alibaba (Beijing) Software Services Co., Ltd., Beijing Baidu Netcom Technology Co., Ltd., Tsinghua University, Beijing Ruilai Smart Technology Co., Ltd., Tianyi Security Technology Co., Ltd.

Company, China Mobile Communications Group Co., Ltd., Xiaomi Technology Co., Ltd., Alibaba Cloud Computing Co., Ltd., Beijing Mianbi Intelligent Technology Co., Ltd.

Ltd., Hangzhou EZVIZ Software Co., Ltd., Beijing Institute of Technology, Beijing Zero One Everything Technology Co., Ltd., Institute of Automation, Chinese Academy of Sciences Institute, Lenovo (Beijing) Co., Ltd., Beijing Qihoo Technology Co., Ltd., iFlytek Co., Ltd., Huawei Cloud Computing Technology Co., Ltd.

Beijing Shuanxing Technology Co., Ltd., the Third Research Institute of the Ministry of Public Security, Ant Technology Group Co., Ltd., Beijing Venusstar Information Security Co., Ltd.

Technology Co., Ltd., Institute of Computing Technology, Chinese Academy of Sciences.

The main drafters of this document are: Xu Ke, Yao Long, Zhang Zhen, Liu Yong, Tan Zhixing, Li Qi, Xie Anming, Xu Xiaogeng, Yang Guang, Cui Tianyu, Hao Chunliang, Zhang Yanting, Xue Zhihui, Guo Jianling, Gu Chen, Jiang Wen, Ye Xiaojun, Tian Tian, Liang Wei, Jiang Weiqiang, Li Jiakun, Peng Juntao, Wang Huadong, Zheng Hongdong, Hong Yanqing, Wang Haitang, Zhu Guibo, Meng Yao, Zhang Xiangzheng, Liu Junhua, Li Fengfeng, Liu Yuhong, Liu Nan, Lin Guanchen, Wang Yan, Luo Hongwei, Tan Yingshui, Zhang Feng, Sun Xudong, Du Jinhao, Xu Shizhen, An Peng, Yu Yang, Sun Yong, Guo Jiexin, Wu Jianliang, Wang Xia, Wang Jinqiao, Gao Boya, Guan Ming, Wang Shijin, Zhao Lili, Wang Wenyu, Ding Zhiguo, Jiang Faqun, Sheng Qiang, and Wu Bowen.

Introduction

Pre-training and optimizing training data are the foundation of generative artificial intelligence and directly determine the quality and security level of generated content.

Pre-training and optimization of training data have security risks in the collection, pre-processing, and use of processing activities, and standards and specifications are urgently needed to improve pre-training Training and optimizing the security level of training data.

Cybersecurity Technology Generative AI Pre-training and optimize training data security specifications

1 Scope

This document specifies the security requirements for generative artificial intelligence pre-training and optimization training data and its processing activities, and describes the corresponding evaluation Price method.

This document applies to generative artificial intelligence service providers to carry out pre-training and optimization training data processing activities and security self-assessment.

It is also suitable for third-party organizations to conduct security assessments on pre-training and optimized training data.

2 Normative references

GB/T 35273

GB/T 41479-2022

3 Terms and definitions

The following terms and definitions apply to this document.

3.1 [Source. GB/T 45654-2025, 3.1]

Use generative artificial intelligence technology to provide the public with services that generate text, images, audio, video and other content.

3.2 Service Provider serviceprovider

Organizations or individuals that provide generative artificial intelligence services in the form of interactive interfaces, programmable interfaces, etc.

3.3 Service User serviceuser

Organizations or individuals using generative AI services.

3.4 pre-training

The training process of using large-scale data to enable generative artificial intelligence models to acquire general knowledge.

3.5 Fine-tuning

Based on pre-training, the training process uses specific domain data to enable the generative artificial intelligence model to acquire domain-oriented service capabilities.

Note. Specific areas are not limited to a certain professional field and usually cover multiple fields.

chinastandards.org - PREVIEW