ZTE Privacy Protection White Paper

COMPLY WITH LAWS | BUILD TRUST TOGETHER |

VALUE BUSINESS ETHICS

2025

ZTE

Statement

Content: This document serves as a reference for stakeholders to understand the privacy protection of ZTE. Unless otherwise agreed, all statements, information, and suggestions herein do not constitute any express or implied warranty. Due to the upgrade or adjustment of products or services, continuous optimization of the compliance system, or other reasons, ZTE has the right to add, modify, delete, invalidate, or occasionally update the content of this document. If you have any inquiries or questions about this document, please contact us via Privacy@zte.com.cn.

Preface

As a global leading provider of integrated ICT solutions, ZTE provides innovative technologies, products, and solutions for telecom operators, governments and enterprises, and consumers across the world.

As a "driver of digital economy", ZTE is committed to speeding up digital transformation across various industries to achieve win-win collaboration with partners in the digital era.

Attaching great importance to **privacy protection**[1], the company strictly complies with the applicable privacy protection laws and regulations of the countries and regions where it operates. For ZTE, privacy protection is not only required by laws, but also acts as the building block of trustworthy and ethical business conduct.

Focusing on specific scenarios, ZTE has built and implemented a privacy protection system with advanced tools, incorporated the system into business processes, and conducted effective supervision to continuously improve its privacy protection capabilities and fully meet relevant requirements.

ZTE incorporates privacy protection into the processes of product design and service delivery, takes privacy protection as an essential element of its core competence and values, and works together with stakeholders to achieve sustainable development while meeting compliance requirements.

ZTE actively engages with industry partners, and makes proactive efforts, including holding forums, releasing achievements, providing suggestions, and participating in standards formulation, to promote privacy protection in the digital era.

[1] Privacy protection, also known as "data protection," refers to "personal privacy protection," "personal data protection," or "personal information protection" in this document.

Contents

ZTE Privacy Protection White Paper (2025)

1 Privacy Protection Policy

With the development of the digital economy and the rise of new technologies, the demand for data has been increasing. Privacy protection has become a popular topic widely discussed among the public, consumers, legislatures, and supervisory authorities, and subsequently, privacy compliance has become a major focus of various industries. As a global leading provider of integrated ICT solutions, ZTE always attaches great importance to privacy protection. The company has established the privacy protection policy of "meeting legal requirements, preventing and controlling business risks, winning customers' trust, and promoting the co-building of a favorable ecosystem", and built an end-to-end privacy protection compliance system that is both closed-loop and process-based.

1.1 Vision for Compliance

Privacy protection compliance aims at guaranteeing privacy security, system stability, user trust, and business freedom.

ZTE strives to build and continuously improve an independent, effective, and efficient privacy protection compliance system which aims to adopt advanced technical and managerial measures to ensure the security and reliability in processing personal information across its entire lifecycle; adapt to changing laws and regulations, as well as technological advancements to ensure sustainable privacy protection practices; earn the trust of customers and users through a commitment to transparency and responsible actions; and safeguard the steady business development and create a virtuous circle of compliance that creates value.

ZTE also strives to improve the effectiveness and efficiency of privacy protection and aims to be a global pioneer and practitioner of privacy protection through all these efforts.

1.2 Mission for Compliance

The privacy protection compliance system is applied to support risk control, trust enhancement, brand building, and value transformation.

ZTE continuously integrates the risk control, trust enhancement, and brand building for privacy protection, so that it not only focuses on respecting laws and regulations, but also embeds compliance into business processes and brand building, and gains greater customer trust through compliance. In terms of risk control, the company complies with applicable laws, fulfills compliance obligations, and focuses on potential risks. ZTE responds to risk incidents in an agile, scientific, and professional manner. As for trust enhancement, the company proactively obtains international certifications, carries out exchanges with customers, and demonstrates compliance capabilities in product R&D, project bidding, and service guarantee, to enhance competitiveness and gain the trust of multiple parties. Regarding brand building, ZTE respects digital and privacy ethics, and emphasizes the privacy protection of users, customers, and employees as part of its corporate values, improving their recognition in ZTE's privacy protection efforts and strengthening the corporate brand.

ZTE consistently adheres to the philosophy of "Compliance Creates Value" and transforms compliance capabilities into value creation capabilities. Specifically, ZTE delves into innovative compliance solutions while actively learning from first-class compliance practices. Based on global risk management, ZTE makes great efforts to turn compliance investment of business units into customers' trust in its products and services, that is, to obtain "positive feedback" from markets throughout the "positive cycle" of compliance building.

1.3 Compliance Objective

1.3.1 Compliance with Legal Requirements and Risk Prevention and Control

ZTE continues to strengthen the identification of privacy protection obligations and conversion of relevant rules in a risk-oriented manner. While complying with the laws and regulations, the company considers the industry's characteristics and its own situation, and fully integrates privacy protection compliance with the corporate governance system. In addition, ZTE learns from first-class privacy protection practices in the industry to ensure that privacy protection risks are visible, preventable, and controllable, thereby laying a solid foundation for compliance management.

1.3.2 Incorporation of Compliance Requirements into Business Activities and Trust Enhancement with Continuous Compliance

ZTE actively responds to the privacy concerns of users and all stakeholders, and continues to promote the effective implementation of compliance requirements in business activities. ZTE embeds compliance control points into business processes, provides general and targeted compliance training for employees, and strictly implements compliance requirements and audits, so as to ensure that all employees respect rules and external parties trust the company's compliance efforts, and that the privacy compliance system is effective and sustainable.

1.3.3 Promotion of Business Sustainability and Pursuit of Digital Ethics

ZTE adheres to compliance-based business sustainability and pursues privacy ethics in a digital world. The company continues to optimize OPEX and compliance efficiency, protect the interests of users, customers, partners, suppliers, shareholders, and employees with a strong sense of social responsibility and excellent privacy protection capabilities, and work with all stakeholders to maintain a sound ecosystem for privacy protection in the industry chain.

1.4 Compliance Guarantee

1.4.1 Tone from the Top and Resource Investment

The management of ZTE attaches great importance to privacy protection compliance—incorporates privacy protection into the company's compliance strategy, and regards data compliance, export control compliance, and anti-bribery compliance as ZTE's three key fields of compliance, to ensure the effective implementation of compliance requirements in business processes. With the tone from the top, ZTE continues to invest

resources in its internal regulations, processes, mechanisms, management, technologies, and tools, and introduce services from law firms and consulting institutions, thereby accumulating profound compliance knowledge and experience and strengthening capabilities.

1.4.2 Well-Structured Organization and Capability Development

ZTE has established a compliance management organization under the leadership of the Compliance Management Committee to perform compliance management from the top down and across business fields, thus effectively communicating compliance ideas and policies to the front line. With a unified compliance organizational structure, the company promotes the accurate understanding of privacy protection compliance requirements and strict implementation of the relevant regulations and processes through continuous compliance training and compliance capability development. The purpose is to guide the fulfillment of compliance requirements, provide timely compliance consulting, and effectively implement compliance measures.

1.4.3 Cultural Integration and Creation of a Sound Environment for Compliance

ZTE has created a sound environment for all parties to participate in compliance work. Specifically, under the guidance of a professional compliance culture that emphasizes "uphold professionalism, pursue mutual growth, embrace challenges, and seek truth and pragmatism", the Data Compliance Dept. continuously optimizes control processes, and enhances integration and interaction with business development. Upholding the philosophy that "Compliance Creates Value", all employees fully disclose, continuously prevent, and collaboratively tackle various risks, take the initiative to provide reasonable suggestions, and participate in the building of the compliance management system.

1.4.4 Reconstruction of IT Systems and Introduction of Tools

ZTE actively adopts advanced technical measures for privacy protection, and promotes the digital transformation of compliance management through the reconstruction of IT systems and introduction of professional tools. Focusing on the key control points of the main business and product R&D process, ZTE continuously strengthens IT-based construction, and introduces IT systems, professional tools, and technical solutions to ensure that all procedures of data processing can be recorded, queried, traced, and verified, thus achieving more systematic, data-based, and intelligent privacy compliance review and risk tracking.

2 Privacy Protection Framework

ZTE has established a risk-oriented compliance management system for privacy protection which is grounded in risk identification and regards compliance management as a tool. The system is built from the top down and promotes the scenario-based formulation of rules from the bottom up, to ensure that compliance rules are incorporated into specific business operations and the system aligns with actual business practices.

The company's management gives high priority to privacy protection. ZTE has aligned privacy protection compliance with its corporate development strategy, and specified the objectives and long-term plans for privacy protection compliance management. By studying

mature models and drawing on great experience in the industry, ZTE has not only effectively prevented privacy protection risks, but also met the expectations and requirements of stakeholders.

ZTE has formulated company-level privacy protection rules that are in line with the *Personal Information Protection Law of the People's Republic of China*, the *General Data Protection Regulation* (GDPR) of Europe, and other applicable privacy protection laws and regulations around the globe. ZTE implements special and exemplary governance for key business and countries respectively, and incorporates privacy protection requirements into product design, service delivery, and operations management to promote the integration of compliance management with business operations and support product innovation through compliance.

2.1 Organizational Structure

ZTE has established a collaborative working mechanism for privacy protection compliance. Under the guidance of the Compliance Management Committee, the Data Protection Officers (DPOs), Data Compliance Dept., and BU compliance teams are responsible for formulating and implementing compliance management requirements; and the Compliance Audit Dept. takes charge of audits and investigations.

As the highest-level organization in the compliance management system, the Compliance Management Committee is responsible for making decisions on major issues of data compliance and providing guidance accordingly. With the focus on the identification of legal requirements, the Data Compliance Dept. researches and interprets global data protection laws and regulations, policies, and rules, plans and formulates, and implements privacy protection compliance strategies and rules as well as conducts supervision, and assesses and reviews compliance risks in specific business processes. The BU compliance teams focus on the feasibility of compliance rules and the optimization of management costs, promote the implementation of compliance rules, and evaluate the necessity and reasonableness of the rules. To strengthen risk control and eliminate blind spots uncovered by the rules, the Compliance Audit Dept. has developed multiple reporting channels to encourage employees to report violations, while conducting audits and investigations, and giving penalties to violators accordingly.

2.2 Rule System

ZTE has established the data compliance rule system, which consists of the compliance policy, *ZTE Compliance Manuals for Data Protection - Corporate-Level Manual*/regulations, scenario-based guidelines.

2.2.1 Policy

The compliance policy refers to a series of documents established in accordance with ZTE's overall business strategy, which specify the redlines that shall never be crossed in business activities. The establishment of the policy demonstrates ZTE's determination to comply with data protection laws and regulations of countries and regions where ZTE operates, and reflects the support of the Board of Directors and the Compliance Management Committee for privacy protection compliance. The policy serves as a guidance for ZTE to carry out data protection compliance.

2.2.2 Corporate-Level Manual/Regulations

The *Corporate-Level Manual*, formulated based on external laws and regulations and ZTE's compliance policy, is a guiding document for ZTE to carry out data protection compliance activities at the company level, including general data protection compliance requirements and key control points. Regulations specify detailed requirements of key control points, or the requirements that are formulated separately based on the ever-changing external laws and regulations so as to convert the key obligations in the external laws and regulations into internal compliance requirements.

2.2.3 Scenario-Based Guidelines

The scenario-based guidelines are a collection of privacy protection compliance documents that define scenario-based requirements for business fields in a more detailed way in accordance with the *Corporate-Level Manual* and regulations. Formulated based on the business structure, the scenario-based guidelines have been launched on the digital collaboration platform for easy access by employees and timely update, thus ensuring the rules are visible, transparent, enforceable, and easy to learn.

2.3 Process Mechanism

ZTE develops IT systems for its key obligations in the processing of personal information and incorporates the systems into business processes to facilitate cross-departmental collaboration and automatically keep complete records that can prove the effectiveness of the compliance management system.

2.3.1 Privacy by Design and Privacy by Default

ZTE formulates appropriate Privacy by Design (PbD) strategies based on system functions and personal information protection requirements of products. The PbD requirements cover the entire lifecycle of personal information, including collection, transmission, storage, usage, sharing, and destruction. The PbD requirements of products cover the entire product life cycle, including demand analysis, design, development, testing and review, launch and deployment, and O&M management.

2.3.2 Data Protection Impact Assessment (DPIA)

ZTE uses the DPIA System to evaluate new products, new technologies, and major changes and sensitive personal information processing in products and services online, thus ensuring the compliance of personal information processing activities that have a significant impact on individual rights and interests. For example, in the demand analysis and product design of R&D process, ZTE assesses the necessity of collecting personal information and analyzes the privacy protection measures taken for permissions, logs, encryption, anonymity, etc. Before personal information processing and transmission, ZTE checks whether relevant security and compliance requirements are met and corresponding compliance measures are taken to reduce risks.

2.3.3 Compliance Controls over Data Extraction

ZTE has established a control mechanism for back-end data extraction. The mechanism requires screening the personal information to be extracted and taking masking or shielding measures for high-risk data before extracting back-end data from systems based on reasonable and necessary business demands. This can effectively reduce the security risk involved with data extraction.

2.3.4 Compliance Controls over Cross-Border Data Transfer

When ZTE carries out business activities involving cross-border transfer of personal information, it will adopt adequate and appropriate mechanisms to safeguard cross-border data transfer, such as satisfying the regulatory approval/filing requirements of the data exporting country, signing agreements related to cross-border transfer of personal information, obtaining the consent of data subjects, and conducting impact assessments of cross-border data transfer.

Actively responding to the requirements of laws and regulations, ZTE is one of the first enterprises to apply for and pass the Security Assessment for Data Export. ZTE has also established a screening mechanism for cross-border transfer of personal information, and adopted necessary measures to strengthen legality of transferring personal information across borders in accordance with laws and regulations.

2.3.5 Compliance Controls over Entrusting Third Parties with Data Processing

If ZTE cooperates with a third party in the processing of personal information, ZTE will conduct risk assessment in accordance with the business type and relevant scenario, and adopt different control measures according to the risk level.

Before a third party is entrusted to carry out personal information processing activities during the business process, a personal information processing agreement will be signed which clearly stipulates the purpose, period, method of processing, types of data, protective

measures, and the rights and obligations of both parties. The department responsible for communicating with the third party will fulfill the supervision obligation.

2.3.6 Response to Requests of Personal Information Subjects

ZTE has provided IT-based, easy-to-use, and open channels for personal information subjects to apply for exercising their rights, so as to ensure that their requests are promptly accepted and comprehensively managed. With the collaboration of privacy compliance experts, DPOs, business leaders, and technical engineers in the response process, ZTE responds to rights and demands of personal information subjects in a professional, objective, and appropriate manner. The whole response process can be automatically tracked and response records can be automatically generated. In this way, ZTE provides convenient interactive experiences for personal information subjects, thereby demonstrating its sense of responsibility and enhancing the public trust.

2.3.7 Response to Personal Information Breaches

By improving its regulations and training, and organizing emergency drills, ZTE ensures compliance with laws and regulations in its personal information processing activities to reduce the probability of personal information breaches. In case of actual, suspected, or potential personal information breaches, the online Personal Information Breach Response System will be applied to implement the whole response process from reporting, judgment, analysis, handling, repair, notification, review to improvement, and to record complete operations to meet such requirements as multi-party collaboration, retrieval of internal documents, and submission of evidence to external parties. Therefore, personal information breaches can be handled in a more scientific, timely, professional, and effective manner.

2.4 Risk Control

ZTE has set up a risk-oriented compliance management system for privacy protection to effectively adapt to the ever-changing environment through risk assessment and continuous improvement.

2.4.1 Prerequisites for Data Collection and Processing

When ZTE acts as a data processor that provides products/services directly to individual users, the risk assessment includes:

(1) Whether the purpose of the data processing activities has been checked and recorded.

(2) Whether the data processing activities have a proper legal basis.

(3) Whether the consent of the personal information subject has been obtained and allowed to be withdrawn, and whether the acquisition of the consent is recorded.

(4) Whether the DPIA is conducted as required.

(5) Whether an appropriate agreement is signed with the entrusted data processor or data co-processor involved.

(6) Whether all the data processing activities are recorded in a comprehensive and timely manner.

When ZTE acts as an entrusted data processor that provides products/services to customers and partners, the risk assessment includes:

(1) Whether an appropriate agreement is signed with the data processor to specify the relevant contents.

(2) Whether the personal information processing activities are carried out in strict accordance with the written instructions of the data processor.

(3) Whether the relevant personal information obtained from the data processor is used for marketing and advertising with the consent of the personal information subject.

(4) Whether the data processor is promptly notified when its data processing instructions violate the relevant laws and regulations.

(5) Whether appropriate measures are taken to assist the data processor in meeting compliance requirements.

(6) Whether all the data processing activities are recorded in a comprehensive and timely manner.

2.4.2 Fulfillment of Obligations to Personal Information Subjects

When ZTE acts as a data processor that provides products/services directly to individual users, the risk assessment includes:

(1) Whether the obligations to the personal information subject are specified and recorded.

(2) Whether a privacy notice is provided to the personal information subject.

(3) Whether a mechanism is in place to respond to the personal information subjects' requests for the exercise of their rights.

(4) Whether the personal information subject is given the right to object when automated processing is involved.

(5) Whether the third party with whom the data is shared or who is entrusted with the processing is notified in a timely manner when the personal information subjects' requests for the exercise of their rights are received.

(6) Whether the requests of the personal information subject are responded to within a specified time.

(7) Whether the response to the personal information subject's exercise of rights is fully recorded.

When ZTE acts as an entrusted data processor that provides products/services to customers and partners, the risk assessment focuses on whether it can actively assist the data processor in responding to the requests from the personal information subject.

2.4.3 Privacy by Design and Privacy by Default

When ZTE acts as a data processor that provides products/services directly to individual users, the risk assessment includes:

(1) Whether personal information is collected and processed only within the scope of the purpose.

(2) Whether the quality and accuracy of the data can be guaranteed.

(3) Whether the purpose of data minimization is specified, or whether relevant measures are taken to meet the requirements for data minimization.

(4) Whether the data is deleted or anonymized in a timely manner after the purpose of data processing has been fulfilled; or whether the temporary documents generated during the processing is deleted or destroyed in a timely manner.

(5) Whether a clear personal information storage period is set.

(6) Whether appropriate measures are taken to ensure the safety and accuracy of data storage and transfer.

When ZTE acts as an entrusted data processor that provides products/services to customers and partners, the risk assessment includes:

(1) Whether the temporary documents generated during the processing is deleted or destroyed in a timely manner.

(2) After the completion of the processing activities, whether the personal information is returned, transferred, or disposed of in a timely manner in accordance with the requirements of the agreement, or whether the corresponding proof is provided at the request of the data processor.

(3) Whether appropriate measures are taken to ensure the safety of data storage and transfer and that the data reaches the designated receiving location.

2.4.4 Compliance of Data Sharing, Disclosure, and Transfer

When ZTE acts as a data processor that provides products/services directly to individual users, the risk assessment includes:

(1) Whether the basic information about the two parties, between whom the data is shared, disclosed, or transferred, is specified, especially the jurisdictions of the two parties.

(2) Whether the legal basis for data sharing, disclosure, or transfer is specified, particularly when cross-border transfer is involved.

(3) Whether the data sharing, disclosure, and transfer is recorded in a comprehensive and timely manner.

When ZTE acts as an entrusted data processor that provides products/services to customers and partners, the risk assessment includes:

(1) Whether the basic information about the two parties, between whom the data is disclosed or transferred, is specified, especially the jurisdictions of the two parties.

(2) Whether the legal basis for data disclosure or transfer is specified, particularly when cross-border transfer is involved.

(3) Whether the data processor is informed of the data disclosure requests in a timely manner.

(4) Whether the party that entrusts ZTE with data processing is informed of the selection and change of the third party that processes personal information in advance.

Based on risk assessment methods and compliance control points, ZTE verifies and supervises data processing activities through self-checks, inspections, audits, and investigations to ensure the strict implementation of compliance management requirements and compliance control points. Through dynamic business re-evaluation and risk re-identification, ZTE optimizes compliance rules and adjusts and improves control measures, to promote privacy protection compliance in a comprehensive manner.

ZTE focuses on two aspects, namely business and country, to improve its compliance capabilities. In terms of business, ZTE develops compliance rules for business activities to ensure that the rules apply to its business development. With dynamic tracking of rules in key countries and regions, ZTE translates global rules into the regulations applicable to the company, and applies local rules based on actual situations.

3 Privacy Protection Co-Building

ZTE has been actively promoting the co-building of privacy protection compliance with industry partners. Specifically, the company takes privacy protection as a shared commitment to be agreed upon during cooperation with relevant parties. While ensuring compliance of ZTE's products and services, ZTE has worked together with all parties to build a sound privacy protection compliance ecosystem across industries.

3.1 Internal Co-Building

ZTE's privacy protection system is established under the collaboration of various departments within the company. In addition to the compliance departments, the collaboration with security-related departments is important for internal co-building. ZTE has established a collaborative working mechanism for data security and compliance, namely, gathering experts in data security, technology, compliance, management, and other fields to carry out joint actions on privacy security and compliance governance. The joint actions are aimed at dealing with high-risk business scenarios, such as cross-border transfer of personal information and the development of new technologies, to strengthen privacy security and enhance trust.

3.1.1 Cybersecurity Co-Management

ZTE gives the highest priority to cybersecurity in product R&D and delivery, and implements top-down, risk-based cybersecurity governance that covers supply chain, R&D, delivery, and various functional fields, thus forming a system that guarantees cybersecurity throughout the product lifecycle. The company released its *ZTE Cybersecurity White Paper 2023 - Governance, Conformance, Openness, and Transparency - Practices of ZTE Cybersecurity Assurance*[2] in December 2023, which systematically introduces ZTE's security governance structure and security assurance system, and emphasizes effective governance methods and practices, that is, focusing on in-depth improvements on the basis of product lifecycle security control, including security by design and security by default, third-party component management, incident response, and vulnerability management. The safety management runs through business flows of supply chain, R&D, and delivery, and is effectively implemented and increasingly improved through the continuous iteration of digital systems.

[2] Please download "ZTE Cybersecurity White Paper (2023)" via the path: ZTE Official Website > About Us > Trust Center > Cyber Security.

Adhering to the principle of openness and transparency, ZTE has established cybersecurity labs in China, Italy, and Germany, enabling customers, supervisory authorities, and other stakeholders to easily and transparently verify the security of ZTE's products. By attaching great importance to the vulnerabilities discovered internally and externally, ZTE conducts responsible disclosures based on the opinions and requirements of customers and the related parties, and provides prevention measures and solutions to achieve closed-loop management of the vulnerabilities. Meanwhile, ZTE has set up a reward program to encourage feedback from security practitioners and institutions worldwide on security issues of products and services.

Cybersecurity is closely related to privacy protection. In the global landscape, supervisory requirements for cybersecurity and privacy protection are continuously tightened, and customer requirements are becoming stricter. In the whole process of product delivery, ZTE implements systematic management and technical specifications for customer data protection, ensuring that the products and services provided by ZTE meet the security and compliance requirements of laws and regulations, industry standards, and customer bidding documents. Through the Overseas Compliance Credibility Enhancement Project, ZTE aims to promote both cybersecurity and privacy protection to gain market trust in an open and transparent manner, including actively strengthening communication with customers and supervisory authorities, participating in industry conferences and forums, and publicizing the company's measures and achievements in terms of data security and compliance.

3.1.2 Information Co-Management

ZTE implements end-to-end information management to guarantee the confidentiality, integrity, and availability of information. With a comprehensive information security management system, and archives and document management system, ZTE conducts regular security inspections, and identifies and investigates violations to improve the information management awareness of all employees.

ZTE has launched a project to strengthen personal information security governance to reduce risks of personal information breaches and abuse. The project aims to: 1) Identify the high-risk systems containing personal information, and include the export of personal information on the back-end of the high-risk systems into the scope of internal information security audits; 2) Determine whether to conduct governance of the systems containing personal information which are identified and reported by business units; 3) Incorporate data security governance requirements for data display, export, and exchange into business processes and ensure that the system functions not meeting the requirements are not launched. Through the project, 100% data de-identification governance is achieved in the high-risk systems, and the personal information about the company's employees, customers, and partners is protected in accordance with the requirements of laws and regulations, demonstrating that ZTE has adhered to the philosophy of privacy protection and compliance, gained both internal and external trust, and conducted proactive compliance actions to deeply integrate information management and privacy protection.

Furthermore, the privacy protection mechanism has been established with the information security management process incorporated. Information management is the prerequisite for privacy protection, while privacy protection is a key objective of information management. In the case of a data breach, which may expose the confidentiality defects of IT

systems, and may infringe on the rights and interests of personal information subjects, privacy protection and information management teams shall work together to deal with risk events.

3.2 Co-Building with Customers

By strictly complying with the global privacy protection regulations, business standards, and customer requirements, ZTE aims to protect personal information across its whole lifecycle. The company incorporates privacy protection language specifying data processing roles into business agreements, and actively assumes corresponding responsibilities and obligations, to build a healthy privacy protection environment and practice corporate social responsibilities together.

When acting as an entrusted data processor, ZTE processes personal information on behalf of the customer only for the purposes specified by the customers in written form. Also, the company actively assists customers in meeting their obligations to personal information subjects. For example, the company deletes the temporary documents generated during personal information processing within the specified recording period; returns, transfers, and handles relevant data in a timely manner and by using the safest method possible; and ensures that personal information is safely transferred to the designated recipient through a network with appropriate controls, preventing the occurrence of any data breach.

ZTE proactively provides customers with compliance materials such as world-class external privacy and security compliance certifications, personal information processing records, and compliance audit reports, to prove compliance with the legal and contractual obligations of an entrusted data processor and help customers demonstrate their own compliance. ZTE also actively assists customers in responding to external regulatory requirements. Specifically, the company fully examines legal risks from the perspective of customers, identifies and meets customers' compliance needs, solves their pain points, and provides customers with enforceable integrated solutions for mutually beneficial collaboration and compliance co-building.

3.3 Co-Building with Suppliers

In accordance with the regulations on supplier management, ZTE promotes compliance co-building with suppliers through the incorporation of privacy protection requirements into business activities, advancing the building of the ecosystem of privacy protection compliance together with the upstream and downstream of the supply chain.

ZTE implements compliance controls through key control points, including signing agreements with suppliers and reviewing cross-border data transfer. In the supplier introduction and certification phase, the company implements graded and categorized management, reviews the suppliers' privacy protection capability, and drafts appropriate agreements or clauses to stipulate the rights and obligations of all parties, in accordance with the products or services provided by the suppliers, including data processing agreements or security agreements, compliance recordkeeping, and security audits for key suppliers. For

different business scenarios, ZTE distinguishes between the roles as "data processor", "entrusted data processor", and "data co-processor" in data processing activities to fulfill the corresponding compliance obligations stipulated by laws and regulations. For high-risk scenarios, such as procurement of training data for large AI models, ZTE has set up a separate review process to conduct compliance assessment on procurement requirements related to training data, supplier qualifications, and procurement targets, and requires the signing of a data transaction agreement to ensure that the source of model data is legal and compliant. If there are activities such as personal information sharing, entrusted processing, and transfer between ZTE and its suppliers, the DPIA shall be performed based on the specific situation; and the corresponding controls shall be taken in accordance with the assessment results.

3.4 Co-Building with Partners

ZTE evaluates the data protection compliance capabilities of partners in business activities strongly related to privacy protection. This ensures that the personal information processing activities are legal and compliant.

In a data processing agreement, ZTE and its partners specify their respective roles and responsibilities concerning data protection, and the obligations to be fulfilled when the personal information subjects exercise their rights or data breaches occur. When ZTE and its partners process personal information for the same purpose, both of them act as data co-processors and jointly provide due privacy notices for the personal information subjects. When processing personal information for different purposes, ZTE and its partners are separate data processors who provide due privacy notices for the personal information subject respectively. When sharing personal information with or transferring personal information to its partners, ZTE strictly complies with legal and contractual requirements of data protection.

3.5 Co-Building with the Industry

Adhering to the philosophy of transparency, openness, trust, and cooperation, ZTE keeps abreast of advanced technologies and methods of privacy protection through exchanges within the industry, and enhances its privacy protection capabilities related to products and services, meeting compliance requirements under new technologies, new applications, and new business models.

ZTE maintains active exchanges with supervisory authorities, industry organizations, technical institutions, colleges and universities, and other enterprises about the interpretation of the latest laws, compliance system building, and the privacy protection driven by new technologies. On September 9, 2022, ZTE participated in the Personal Information Protection Forum of the China Internet Civilization Conference hosted by China's Cyberspace Administration and Central Commission for Guiding Cultural and Ethical Progress, and shared innovative practices such as PbD processes, self-developed privacy compliance review system, privacy compliance screening tools for apps, and the building of "dual centers"

for product privacy and user privacy. As a result, ZTE's terminal privacy protection and security compliance competitiveness building was selected as an "innovative practice of personal information protection". On November 16, 2023, ZTE hosted the 4th Multinational Corporation Trade Compliance Symposium. In the sub-forum on compliance management for new technologies, ZTE discussed several topics with industry experts, including compliance challenges and opportunities driven by new technologies, the sci-tech ethics related to AI, and data security compliance in the era of digital intelligence, introduced the key points of privacy protection compliance for generative AI, and shared its own practices in privacy protection compliance. In addition, ZTE has held several forums for scholars on data security and personal information protection, inviting experts from the academia and industry to discuss the trending topics and corporate practices in data compliance.

4 Privacy Protection Practices

4.1 Research on Laws and Regulations

To adapt to the frequent changes in the global data compliance laws, ZTE has formulated a standardized process for dynamic tracking and identification as well as graded response to external rules. With a risk-oriented approach, the company regularly identifies and responds to external regulations, regulatory cases, and industry trends in the countries and regions where it conducts business, providing support for addressing privacy protection risks and converting relevant external rules into internal regulations. For each important external regulation strongly related to its business, ZTE identifies relevant compliance obligations, analyzes the maturity of compliance controls over business activities, and conducts risk assessment. Based on the assessment results, the company incorporates key control points into business processes, integrating the legal requirements for the full life-cycle management of personal information into internal rules. In addition, ZTE publicizes obligations concerning privacy protection compliance to relevant stakeholders and promotes joint implementation.

ZTE has established a privacy protection platform with sufficient legal resources such as Chinese data compliance legislation, global data protection legislation, industry trends, and thematic studies. All of those resources are accessible to business units and compliance teams for information query and capability development. Via the Global Law and Policy Research Institute, ZTE's privacy protection team has converted cutting-edge legal research findings and business experience into multiple research outcomes, such as the *Personal Data: A Conceptual Elucidation, Research on the Establishment of Data Protection Officers in Multinational Enterprises, Key Elements of Compliance System Building, Analysis and Application of Personal Information Management System (PIMS) Based on ISO 27701, Research on Legal Accountabilities for Enterprises and Their Executives Committing Compliance Violations, Research on the Correlation Between Privacy Protection Laws and Privacy by Design Related to Chinese Apps, Empirical Research on IT-based Privacy Compliance, Compliance Challenges for Chinese Intelligent Connected Vehicles Going Overseas, Compliance Practices in Data Resource Procurement,* and *ZTE's Compliance Scheme for Export of Data from China.* These research outcomes provide prospective analysis and strategic recommendations based on actual business situations, offering continuous value and long-term guidance for the company's compliance management.

4.2 Business Practice

As the laws and regulations on privacy protection are frequently updated and published, compliance governance solutions need to be adjusted accordingly. ZTE has established a standardized process for data compliance risk assessment, translated external regulatory requirements into internal compliance requirements corresponding to business activities, removed deficiencies based on feedback from business units, and implemented targeted controls for complex and evolving challenges.

In addition, ZTE encourages each business unit to implement privacy protection rules tailored to their own business characteristics, bringing about a large number of good practices for personal information protection and extensive practical experience. As a result, compliance management is further integrated into business operations, and the company's overall privacy protection capabilities are improved.

4.2.1 Sales and Marketing

ZTE's sales and marketing activities involve marketing, customer relationship management, opportunity management, and bidding management. Scenarios that involve personal information processing include customer relationship establishment and maintenance, visitors from customers, and business exhibitions. In addition, scenarios that involve the signing of agreements with customers to specify data processing rights and responsibilities include solution preparation and bidding, contract negotiation and contract signing, and contract signing review.

In the business scenarios of customer relationship management, the business contact information provided by the customer, such as the name, telephone number, and email address, is mainly processed for daily business communications. Privacy protection and control are implemented through the IT systems to ensure that the collection, storage, and use of personal information comply with the principle of data minimization. In special cases, when a customer is invited to visit ZTE or participate in an exhibition and it is necessary to book a flight or hotel for the customer, if sensitive personal information, such as a passport or ID number, needs to be collected, the company will, in an appropriate way, notify the customer of the purpose of collecting and processing his/her personal information (such as sending a privacy notice), obtain the consent of the personal information subject, and delete the personal information once the activity concludes.

In the business scenario of bidding management, the company actively works with the customer to sign relevant agreements, in which ZTE will fully disclose the data processing purpose, transfer path, data type, and technical and organizational measures for ensuring data security. The company will also proactively fulfill relevant obligations—for example, processing a customer's information only after the customer's authorization is obtained and the internal approval process is completed.

4.2.2 Telecom Product

ZTE's telecom product business involves wireless and computing power products (RAN, intelligent computing, CCN, servers, etc.), wired products (transport network, fixed network, and multimedia products), digital energy products (telecom energy products), and product-related solutions. The cybersecurity and data security settings of the telecom

products directly affect users' personal information security. Therefore, the company attaches great importance to the PbD, fulfillment of personal information subjects' rights, product security reinforcement, and permission management.

In telecom product R&D, ZTE integrates PbD into the High Performance Product Development (HPPD) process. Through rule incorporation and actual practices, including risk identification, solution design, pilot project operation, and specification revision and release, the risk controls for personal information across its full lifecycle is, as a PbD requirement, incorporated into the stages of R&D requirements management, system design, development verification, and product launch. The incorporation of PbD in the R&D projects is checked and accepted during the milestones such as project technical review and version release.

Besides, ZTE conducts DPIAs in the system solution phase of the HPPD process. Based on the identified personal information and data flow, the company identifies potential threats and product vulnerabilities across the full lifecycle of data processing from two aspects, namely protection of personal information subjects' rights and data security, assesses the risk level, determines the risk treatment strategies, and formulates and implements risk treatment plans.

4.2.3 Mobile Device

The mobile device business of ZTE is an end-to-end series of activities including the R&D, design, supply, delivery, sales, and after-sales service of mobile devices. Specific activities include product R&D, product operation, product supply, product sales and customer service, brand management, and quality management.

By sticking to the privacy compliance requirements for mobile device products, safeguarding the company's compliance image, and creating compliance brand value for mobile device products, ZTE's mobile device units strive to present a trustworthy image to its users and the whole community. The units are committed to promoting user experience in terms of ZTE's privacy protection, and providing more secure products and services for users. PbD is incorporated into the full lifecycle of product R&D, and the well-developed organization, process, and technical management system for privacy protection helps ensure that all collected personal information is protected in an all-round manner and processed in accordance with compliance requirements.

To meet the regulatory requirements for privacy compliance, the mobile device BU compliance team, in collaboration with business units, has established a compliance review process for the launch of mobile devices and the pre-installation of apps on mobile devices. Before being launched, mobile devices and their pre-installed apps must undergo a strict privacy compliance review. Any issues identified during the review must be rectified, and compliance risk identification and control are carried out through a three-level approval process involving the business team, BU compliance manager, and compliance expert. From the technical perspective, consumer privacy protection is ensured through measures such as data encryption, anti-breach, and database auditing. For activities other than product R&D, such as e-commerce, supply chain, customer service, after-sales service, research, and crowdsourced testing, comprehensive process management regulations have been designed to ensure that all business operations meet privacy protection requirements.

As the regulation on privacy protection gets tighter, the product security team of the mobile device units has carried out in-depth research on privacy security of products, and has independently developed and applied a detection platform for mobile device privacy security and compliance, namely APIMonitor, realizing closed-loop management from the review process to technical supervision through static and dynamic testing. The R&D and launch of the detection platform has enabled the testing of a large amount of code, thus saving the manpower involved in detection and the expense of purchasing third-party detection tools, and effectively meeting the product-developing units' detection requirements for mobile apps. In addition, the launch of the detection platform testifies to the compliance capabilities of the mobile device units, and reflects the implementation of compliance rules, the commercialization of compliance solutions, and the value created by compliance management.

4.2.4 Supply Chain

ZTE's supply chain business is about integrating upstream, midstream, and downstream resources through the entire management process comprising of the design, planning, control, and optimization of the material, information, and financial flows. In such manner, resource wastes are kept at the minimum level, the company's overall efficiency is maximized, corresponding benefits are given to the members in the supply chain, and the customer demands are rapidly satisfied. Supply chain activities that involve personal information processing mainly include procurement and logistics.

Personal information processing in supply chain activities mainly involve the processing of names, telephone numbers, email addresses of the business contact persons specified by customers and suppliers, to facilitate the business negotiation, bidding, receipt, delivery, and payment. When collecting the personal information provided by suppliers, ZTE, in a proper way (such as providing the privacy statement or sending emails), informs the personal information subjects of the purpose and other necessary information about data collection and processing, and, when applicable, obtains the consent of the personal information subjects. The company collects only the minimum necessary scope of personal information that is related to the business, and protects the rights of personal information subjects. For example, if a supplier or individual requests access, deletion, or modification of personal information processed by ZTE's Supply Chain, the company will respond in a timely and effective manner. Moreover, the company evaluates the storage period of personal information; after the collaboration with the supplier concludes, the company deletes the personal information provided by the supplier in accordance with external laws and internal regulations. When ZTE stores or transfers personal information provided by a supplier, the company will implement permission management, encryption, and operation log recording on the IT system.

For a procurement contract with a supplier on processing personal information provided by ZTE or its customers or other suppliers, ZTE investigates, audits, and supervises the supplier's capabilities to protect personal information and signs appropriate data compliance agreements with the supplier. After the termination of the agreement, ZTE requires and urges the supplier to delete the personal information in accordance with laws, regulations, and the contract. For recycled devices from customers and the components that are replaced during repair and that may contain the personal information of customers or end-users, the Supply Chain masks or destroys data on the corresponding storage devices to control the risks of

data breaches and improper data processing. If physical processing by the recycler is required, the company requires the recycler to sign the data compliance agreement and provide processing reports, so as to reduce the risks of personal information breaches.

4.2.5 Engineering Service

ZTE's engineering service refers to the activities that are carried out to transfer the sales contracts into deliverables through engineering, technology, and service delivery, so as to generate revenues. The engineering service activities related to privacy protection include technical delivery, customer support, and engineering outsourcing management. The types of involved data include network user data of operators, and personnel information about third-party partners.

In line with the characteristics of business activities in the engineering service field, ZTE's engineering service units formulate scenario-based guidelines for data compliance of engineering service activities, incorporating privacy protection rules into the business scenarios and processes to ensure that the rules can be effectively implemented. The related privacy protection control requirements are publicized to employees through compliance training and publicity activities, so that employees can better understand the necessity and details of related control measures, preventing ineffective implementation due to inaccurate understanding of privacy protection requirements. In addition, the engineering service units focus on the high-risk business scenarios and processes by establishing a key control point inspection mechanism for privacy protection applicable to the engineering service field, and inspect and evaluate the implementation of the key control points in related business activities, thus ensuring the effective implementation of the key control points. By analyzing the inspection results, collecting and giving feedback on the employees' suggestions on the implementation of the key control points, and obtaining audit recommendations from external institutions, the engineering service units review the reasonableness of setting the key control points, and optimize their setting and implementation modes in a timely manner, so as to continuously improve the control effectiveness and reduce the costs of rule implementation while ensuring that the key control points cover the major compliance risks of privacy protection in business activities.

4.2.6 HQ Functional Business

ZTE's HQ functional business includes the operations management of the company, and the administration affairs and real estate services that support the productivity of the core business.

Given the wide range of business and a large number of activities in HQ functional business, the company mainly adopts a scenario-based approach to manage personal information collection and processing, and cope with the risks involved in different scenarios on a case-by-case basis. For privacy protection in the HQ functional business, assessments are conducted on various aspects, namely the basis of the legality, consent obtaining methods, necessity of information collection, minimization of the purpose and authorization scope, third-party suppliers' security, reasonableness of retention periods, and IT system security. Based on the assessment results, specific control suggestions are provided for risky scenarios.

Take the international third-party customer satisfaction survey for example—its aim is to improve ZTE's services and products based on customer feedback gathered through the questionnaire, and thus enhance customer satisfaction. Based on the principle of purpose limitation, the purpose and time period of using the customers' information are stated in the survey; to ensure the minimization of the authorization scope, the scope of people with access to the information on survey respondents, the amount of such information stored, and the scope of receivers of such information are limited to the minimum range; to ensure transparency, the customers are informed of the personal information that is transferred, the processing principles, and their rights; and to ensure confidentiality, the personally identifiable information is strictly kept confidential during the survey and is not passed to any third parties.

4.2.7 Human Resources

ZTE's human resources business is a series of activities related to the Human Resources Management (HRM), including human resource planning, recruitment and staffing, appointment management, administration of management members, performance management, corporate culture, compensation management, employee relationship, learning and capability development, and health and safety. HRM activities involve the processing of a large amount of personal information of employees. ZTE highly respects the personal rights and interests of employees and protects their privacy. The company has incorporated the requirements of applicable laws into corporate governance regulations, and translated Chinese and international standards into practical management measures. In this way, the company ensures that the employee information is processed in a secure, credible, compliant, and lawful manner. ZTE is committed to promoting its employer brand, building a mutually trusting relationship with employees, and shaping an image as "employee privacy defender".

Privacy protection has been integrated into the entire process of ZTE's human resources business. Through organization building, regulation formulation, process improvement, and technical protection measures, the company ensures the personal information of employees and related parties is collected and processed in a secure and compliant manner. The privacy policy has been incorporated into the IT systems related to human resources activities, clearly specifying the types of information to be collected, legal bases, rights of the personal information subjects, and ways to exercise such rights. In addition, the aforementioned systems have met ZTE's baseline requirements for product and information security in the phase of requirement analysis, development, testing, version release, and launch. For offline activities that may involve the collection of personal information from employees or their family members, privacy notices will be issued to ensure that the employees and their family members fully understand the purpose of data collection and use.

Take "We Love ZTE" for example, which is a teambuilding activity for employees and their family members. Through such activity, ZTE aims to improve the family members' sense of recognition and support for the employees' job. While providing the family members with desirable services, the company follows the principle of data minimization in collecting their ID numbers and food habits, and specifies the types of the information to be collected and relevant purposes in the privacy notice. Besides, all information is retained in the company's encrypted document library, which is accessible to only relevant personnel of the activity organizer. After the activity, the electronic personal information is deleted in a timely manner, and related paper documents are destroyed to ensure that the processing of personal

information about employees and their family members complies with the laws, regulations, and policies of the countries and regions where the company conducts business.

4.2.8 Finance and Accounting

The finance and accounting business of ZTE refers to the overall financial management of the company, which includes financial accounting, treasury management, tax management, budget management, cost management, financial performance management, receivables management, financial supervision, sales financing, external guarantee, and securities affairs. The business activities in the finance and accounting field mainly involve the employees and external partners of the company, and the processed personal information is highly sensitive, involving financial data, identity information, and tax matters. Therefore, in information-disclosure scenarios such as expense reimbursement, individual income tax declaration, and securities affairs, personal information shall be protected in an all-round manner to safeguard the personal rights and interests of the employees and external partners.

Adhering to the privacy compliance requirements for finance and accounting activities not only protects the personal privacy of employees and external partners, but also helps maintain the company's compliance image. The finance and accounting units are committed to enhancing the internal and external users' awareness of privacy protection, and keep providing secure and credible products and services for users. They also incorporate the concept of privacy protection into the entire process of financial services, and guarantee compliant processing of personal information through desirable organizational and structural measures, formulation of regulations and processes, and technical methods.

Take expense reimbursement for example: ZTE uses the Finance Online (FOL) system for expense reimbursement. To meet the privacy compliance management requirements, a mechanism is established for the review and release of the privacy policy on the FOL system. In the FOL system, the transmission and storage of personal information are strictly controlled via permission management, and security hardening is conducted. Regarding the IT system-based cross-border transfer of personal information between ZTE's headquarters and an overseas ZTE subsidiary due to the subsidiary's daily operation and management needs, the headquarters will sign a data transfer contract with the subsidiary to ensure compliance in the cross-border information transfer.

4.2.9 Strategy and Investment

The strategy and investment business of ZTE refers to the overall strategic planning and investment management of the company. Strategy and investment activities include mergers and acquisitions, establishment of new entities, divestment or equity sales, entity dissolution, entity transformation, cooperation with external parties, and exhibition events. The strategic and investment business involves the processing of personal information, mainly in the context of exhibition activities, mergers and acquisitions, equity sales, and entity dissolution.

An exhibition activity involves inviting customer representatives and arranging participants' trips, accommodation, and reception necessitating the processing of a large amount of personal information. Therefore, the privacy protection in exhibition scenarios is an important part of ZTE's privacy protection efforts. For example, during the MWC Barcelona, a major international exhibition in the ICT field, ZTE implements privacy protection compliance

controls throughout the exhibition process, effectively protecting customers' personal information. Before the exhibition, the company sends a privacy notice to customers along with the invitation letter. The notice specifies the types of personal information to be collected and the corresponding purposes, the protection measures, the rights of the customers, and the ways to exercise such rights. During the exhibition, in addition to the business personnel, the BU compliance manager and the data compliance experts provide real-time support for the exhibition in terms of privacy protection and data compliance, offering comprehensive personal information protection for all the participants.

On the one hand, the data owned by an enterprise may be used for different purposes and generate varying value; On the other hand, the collection, use, and sharing of such data may bring risks of different degrees to the enterprise. Based on the requirements of Chinese privacy protection laws on mergers, divisions, dissolutions, bankruptcies, etc., ZTE has outlined the privacy protection risk control rules for investment and financing business; and has formulated the *Data Compliance Guidelines for Investment and M&A, Data Compliance Guidelines for Sales of Subsidiaries,* and *Data Compliance Guidelines for Liquidation and Deregistration of Subsidiaries* based on actual business processes, and implemented them in projects to effectively control the compliance risks related to privacy protection in investment and financing activities.

4.3 Openness and Sharing

ZTE is committed to sharing achievements and promoting exchanges and cooperation. Through forums, seminars, publications, and self-media, ZTE stays updated on the latest regulatory changes, actively shares its privacy protection practices and compliance governance experience with other enterprises, professional organizations, universities, and institutes, and participates in in-depth communication with industry professionals, aiming to advance mutual development and jointly build a credible compliance environment.

With its official WeChat account, "All About Compliance", ZTE presents the latest trends in data compliance, provides a platform for research on the laws across countries, addresses the pain points of compliance governance within the industry, and shares valuable insights into privacy protection. With the account, the company has published multiple articles, including the *White Paper on Compliance Governance of Cross-Border Data Flows*, *ZTE 5G Application Scenarios and Privacy Protection Research Report, Employee Privacy Protection Practices, EU AI Act: World's First Comprehensive AI Law, Analysis and Suggestions on Potential Data Protection Risks of ChatGPT, Identification of Data Privacy Compliance Obligations in AIGC R&D and Application—A Case Study on Italy's Regulations Concerning ChatGPT, A Complete Introduction to GDPR Jurisdiction, Compliance Requirements for Internal Investigations of Enterprises under the Personal Information Protection Law of the PRC, and Data Compliance in Plain Language, receiving positive responses* and building a strong reputation in privacy protection compliance.

ZTE regularly compiles internal legal research results and shares them with the public. For example, it has released multiple cutting-edge and practical research reports on privacy protection, such as the *White Paper on Compliance Governance of Cross-Border Data Flows*, *ZTE 5G Application Scenarios and Privacy Protection Research Report*, *PbD Research*

Report, *Global Data Protection Authorities Pocket Book*, and *White Paper on Cases of GDPR Enforcement,* demonstrating its commitment to fostering an open and collaborative privacy protection culture.

4.4 Key Certifications

Strong capabilities provide the guarantee for privacy security. ZTE prioritizes privacy protection for its products and services, and continuously strengthens physical, managerial, technical, and organizational safeguards against data security violations, striving to create a sustainable, transparent, open, and trustworthy privacy protection environment.

ZTE has continuously obtained authoritative certifications in the industry. For example, ZTE has obtained the ISO/IEC 27701:2019: Privacy Information Management certification for various business sectors, including mobile devices, 5G, CCN, digital technology products, and HRM. In addition, the company's mobile device business has obtained the ePrivacyseal Global issued by ePrivacy GmbH, an authoritative privacy certification body in the EU. These authoritative certifications indicate that ZTE provides standardized, mature, and comprehensive privacy and security guarantees to users worldwide.

ZTE's 5G product line has passed the development and product lifecycle audits of the continuously iterative Network Equipment Security Assurance Scheme (NESAS) of the GSMA multiple times, and the company's 5G RAN and 5GC products have passed the NESAS security assessments. Additionally, the company's 5G NR gNodeB products have received the NESAS Cybersecurity Certification Scheme - German Implementation (NESAS CCS-GI) certification, issued by the German Federal Office for Information Security (BSI). In addition, ZTE's 5G RAN solutions, the full range of OTN products, and data communications products have successively obtained the Common Criteria (CC) EAL3+ certification, and the 5G base station software has obtained CC EAL4+ certification. All these achievements demonstrate ZTE's dedication to providing secure, reliable, and compliant telecom products and solutions for global customers.

5 Major Events

Passed Authoritative Certification or Assessment	
China's Data Management Capability Maturity Assessment Model (DCMM) - Level 5 Certification (highest level)	Oct. 2024
EU's ePrivacyseal Global	Jun. 2024
ISO/IEC 27701:2019: Privacy Information Management	May. 2024
Data Export Security Assessment by the Cyberspace Administration of China (CAC)	Jan. 2024
U.S. TRUSTe Enterprise Privacy certification	Aug. 2022
Awards and Honors	
"ZTE: Improving Enterprise Resilience and Building a Best-in-class Compliance System" Won 2024 Ram Charan Management Practice Award - Award of Excellence	Oct. 2024
Security and Privacy Pioneer Award from the British Standards Institution (BSI)	Dec. 2022
"Innovative Case of Personal Information Protection" in 2022 China Internet Civilization Conference	Sep. 2022
"Pioneering Practice of Compliance Audit for Personal Information Protection" at the first Digital Audit Forum hosted by the China Academy of Information and Communications Technology (CAICT)	Jul. 2022
Privacy Strategy Contribution Award from the BSI at the 3rd Smart Summit Economic Forum	Jan. 2021
Branding	
Included privacy protection as a product highlight of Nubia Z50, a flagship model	Dec. 2022
Included privacy protection as a product highlight of Axon 40 Ultra, a flagship model	Nov. 2022
Launched ZTE's official Privacy Center on its website	Nov. 2022
Released the slogan "Your Privacy, Our Priority" and the logo of privacy protection for mobile device products	Jul. 2022
Internal Self-Developed Compliance Management Platforms	
Intelligent Data Screening (IDS) system	Jul. 2024
Data Compliance System (DCS)	Dec. 2023
Privacy Compliance Review System (PCRS)	Oct. 2022
App Privacy Compliance Screening Tool	Oct. 2022

Acknowledgement

This white paper is jointly compiled by ZTE experts in various fields.

Our heartfelt thanks go to Huang Zhimin, Yang Yuxin, Xu Min, Mei Aoting, Fang Yuan, Liang Chujun, Zhang Danyan, Guo Piaoyang, Liang Yanshan, Jiang Lu, Li Huahong, Li Aotian, Qu Shenwei, Chen Lisheng, Li Lin, Wen Hualong, Lei Sujun, Chi Yifei, Zhang Qinwei, Xue Yusong, Zhou Shuyao, Lu Kexing, Yue Yanhong, Wang Zongping, Hu Zhiqiang, Chen Zhengwei, Zhang Liang, Deng Yuanyuan, Chen Weite, Ren Ziqian, Zhang Ji, Tang Dandan, Huang Zhiyu, Xia Meng, Wu Chanyuan, Guo Qian, Li Nan, and other related personnel for their great efforts and support.

ZTE Privacy Protection White Paper

COMPLY WITH LAWS | BUILD TRUST TOGETHER | VALUE BUSINESS ETHICS

ZTE