ZTE Privacy Protection White Paper

COMPLY WITH LAWS | BUILD TRUST TOGETHER | VALUE BUSINESS ETHICS

2020

ZTE

Statement

Content Statement: This document serves as a reference for interested parties to learn about the privacy protection requirements of ZTE Corporation. Unless otherwise agreed, no express or implied guarantee is given in all statements, information and suggestions in this document. The content in this document may be modified due to product or service upgrade, adjustment or other reasons. Due to the continuous optimization and improvement of the compliance system, we have the right to add, modify, and delete the content of this document and update it irregularly. If you have any inquiries or questions about this document, please contact us via Privacy@zte.com.cn.

Preface

As a global leader in telecommunications and information technology, ZTE has comprehensive end-to-end product lines and provides integrated solutions in the telecommunications industry. By means of all series of wireless, wireline, and terminal devices and professional telecommunications services, ZTE is capable of satisfying the diversified requirements of global operators, government and enterprise network customers, thus promoting rapid innovations. ZTE has been committed to providing integrated end-to-end innovations and solutions including voice, data, multimedia, and wireless broadband to deliver excellence and value to consumers, including carriers, businesses and government and enterprise network customers, from over 160 countries worldwide to enable increased connectivity and productivity.

ZTE attaches great importance to privacy protection. In accordance with the *Cybersecurity Law of the People's Republic of China*, the European Union's *General Data Protection Regulation* (GDPR), and other applicable privacy protection laws and regulations of countries and regions across the world, ZTE has established a well-designed compliance system and conducted systematic risk control. For ZTE, privacy protection is not only a legal requirement, but also the building block of trustworthy and ethical business conduct. [1]

The privacy protection compliance architecture of ZTE focuses on core scenarios and operates efficiently. ZTE builds an end-to-end, process-oriented and closed-loop privacy protection compliance system to

[1]Privacy protection, also known as "data protection", refers to in this document as being consistent with "personal privacy protection", "personal data protection", "personal information protection", and etc.

comprehensively protect personal privacy and fully protect personal data security.

ZTE incorporates privacy protection into the process of product design and service provision, takes privacy protection as an essential element of the company's core competence, and works together with customers, suppliers and other partners to achieve excellence and sustainable development compliantly.

ZTE also actively communicates with other companies in the telecommunications industry, regularly organizes privacy protection compliance forums, publishes research results, actively participates in the establishment of standards and regulations related to privacy protection, and contributes to the development of privacy protection compliance.

Contents

ZTE Privacy Protection White Paper

(2020)

1 Privacy Protection Compliance Strategy

With the development of privacy protection legislation and law enforcement in the world, the telecommunication industry has gradually become the focus of privacy protection because its extensive coverage of new infrastructure construction involves a large group of individual users. To effectively promote privacy protection compliance, ZTE has established the privacy protection compliance strategy of "meeting the compliance requirements, fully preventing and controlling risks, promoting compliance implementation in business, building trust together, ensuring the sustainable development of business, and building a favorable compliance ecosystem together".

1.1 Compliance Vision

Establish an applicable, effective and leading privacy protection compliance system.

Tailored to the features of the telecommunications industry, the privacy protection compliance system of ZTE has been adapted to fit the internal risk preferences and external regulations. ZTE is committed to establishing applicable rules, conducting effective publicity, guaranteeing full implementation of requirements, and performing audits independently. The company aims to incorporate compliance requirements into business processes that are well-functioning and keep risks under control. In the privacy protection field, we endeavor to become the pioneer and paradigm in corporate compliance in China and globally.

ZTE complies with applicable regulations, fulfills compliance obligations, eliminates potential risks, prevents and controls the occurrence of regulatory penalties and judicial proceedings, and effectively responds to and handles risks. We actively carry out external certification, demonstrate compliance capability in product approval,

project bidding, customer audit and compliance inquiries, remain competitive in the market, and win customers' trust. We adhere to the ethics of privacy in the era of the digital economy and incorporate data protection into our values to secure the privacy of customers, users and employees. Data protection is our building block of ethical business conduct.

1.2 Compliance Mission

Privacy protection compliance and control, increased market trust and brand creation.

To ensure that risks can be accurately identified, controlled and managed, the privacy protection statement of ZTE is based on the law, complies with the rules, and is incorporated into the business so that ZTE can gain trust from the customers and integrate compliance into our corporate value to define our brand image. Through overall coordination, active planning, challenge taking, risk management and control performing, and compliance schemes and business practices exploring, ZTE receives positive feedback of compliance implementation after introducing compliance into our business, completing a virtuous cycle.

In terms of rules, ZTE focuses on the key business and core scenarios. Under the guidance of employees in key positions, ZTE interprets the complex rules into plain words which can be easily accessed, learned and shared among employees. Thus, rules can be implemented in the frontline business units effectively to ensure the consistent and effective implementation of the rule system.

In terms of support, ZTE takes in the perspective of business units, cuts the cost while keeping the efficiency of compliance management, and controls investment to avoid duplicated work. Through the compliance training conducted level by level, the rules can be delivered to all business units, which enables them to independently evaluate risks and implement compliance requirements.

In terms of management, a matrix is used to plan, implement and evaluate the risk control system, which simplifies the process of risk control. ZTE implements management and control points through IT-based tools, reducing manual and offline operations and repetitive control.

Privacy protection safeguards value. ZTE provides a stable environment for the market competition through business risk control and risk point reductions. Privacy protection creates value. ZTE ensures the security of user data privacy in terms of design solution selection and security reinforcement. Thus, we earn trust from the customers.

1.3 Compliance Objective

1.3.1 Meeting the compliance requirements and fully preventing and controlling risks

ZTE adheres to the business ethics and abides by the laws and regulations of the location where the business is carried out. Facing the increasingly stringent legislation and law enforcement of the global privacy protection compliance, we comply with the requirements of the location where the business is carried out in accordance with the local privacy protection laws and regulations. We fully respond to the customer privacy protection audit, effectively respond to the global data supervision and review, prevent and control the privacy protection risks, and lay a solid foundation for the privacy protection compliance construction.

1.3.2 Promoting compliance implementation in business and building trust together

ZTE respects the privacy of the users and protect their privacy-related rights. We continue to promote the effective implementation of the compliance requirements in business activities, explore the working methods for combining compliance management with business practice, and realize the comprehensive implementation of the privacy protection compliance requirements through reasonable rules, comprehensive training, resolute implementation and effective auditing.

1.3.3 Ensuring the sustainable development of business and building a favorable compliance ecosystem together

ZTE ensures the sustainable development of business. We realize the lowest management cost and the highest efficiency with the premise of safe management, protect the interests of customers, partners, shareholders, employees and stakeholders by constructing excellent privacy protection compliance, and work together to build a

favorable compliance ecosystem for privacy protection compliance in the entire industry chain.

1.3.4 Establishing compliance standards and building a leading compliance brand

ZTE establishes standards for compliance and builds a leading compliance brand. We cooperate with experts in the industry to develop in an open and inclusive manner, carry out in-depth discussions with experts in the professional ecosystem of privacy protection compliance , take the leading position in compliance in the industry, and output general achievements, standards, and scenarios. Thus, privacy protection compliance becomes our competitive advantage and contributes to the continuous increase of trust on products and services.

1.4 Compliance Guarantee

1.4.1 Attention from top management and resource investment

The top management of ZTE attaches great importance to privacy protection compliance. Privacy protection compliance of ZTE is incorporated into the company's development strategy. We regards the data protection compliance as one of the three key fields of compliance of ZTE. The other two key fields are export control compliance and anti-commercial bribery compliance, which are of great importance. With the support of the top management, we continue to increase investment in data protection compliance, strengthen cooperation with external law firms and consultants, optimize organizational structures, and increase investment in human resources, especially experts, to ensure the implementation of the privacy protection strategy.

1.4.2 Mature organization and capacity improvement

ZTE has established an end-to-end compliance management system under the leadership of the Compliance Management Committee. We recruit experts to construct a professional team, the Center of Experts (COE), recruit more competitive employees for the full-time Business Unit (BU) compliance team, and set up the Points of Contact (POCs) to deliver the compliance knowledge and policies to the frontline business units. Following a unified compliance organizational structure, the privacy protection units of ZTE and other business units jointly establish a professional security team with hierarchical management, multi-point control, and collaborative work to

implement compliance governance. We achieve the compliance goals through providing continuous compliance training for capability internalization, providing guidance for the implementation of compliance requirements, responding to compliance consultations, and effectively implementing compliance measures.

1.4.3 Business integration and good atmosphere

ZTE has formed a mechanism characterized by active cooperation between business units, employees driven by their own compliance consciousness and incorporation of overall compliance culture. In the process of promoting privacy protection compliance, business units pay close attention to the data processing activities involved in the business, cooperate with the privacy protection compliance departments to carry out risk assessments, actively implement the privacy protection requirements, formulate privacy protection compliance manuals for business fields, optimize business processes in accordance with the compliance requirements, and vigorously promote the dual-cycle development of compliance and business. All employees respect the rules, remain open-minded and implement compliance requirements.

2 Privacy Protection Compliance Framework

ZTE has incorporated privacy protection requirements into product design, service delivery, and management and internal control activities, established a company-level compliance rule system that meets the requirements of the European Union's *General Data Protection Regulation* (GDPR), implements privacy protection governance on key business and key countries, and promotes high integration of business and compliance and corresponding innovative implementation.

ZTE has established the principle of "following applicable laws and regulations and multi-dimensional end-to-end governance", which extends the rights and obligations of data subjects, data controllers and data processors to the operation and implementation of product design, management and internal control, and service delivery to realize the end-to-end governance and implementation of data protection. Thus, we promote the integration and implementation of compliance in the corporate governance system.

ZTE has established the organizational model of "professional team support, lines of defense for compliance control, and collaboration among multiple internal and external entities". ZTE has a full-time data protection officer, and has deployed compliance directors or product security directors at the company's headquarters, in various business fields, and at the subsidiaries to form a vertical, collaborative and complete risk prevention and control operation structure.

ZTE has established a compliance management framework to implement multi-dimensional end-to-end management, which includes elements of attention from top management, governance structure, policies and rules, risk assessment, process control, supervision and inspection, and compliance training and record keeping. The framework ensures the effective operation and continuous improvement of data protection compliance.

ZTE has established a structure of "policy, manuals, norm, and scenario-based guideline" to instruct various business units to identify and respond to data protection risks in business activities based on scenarios. Through the establishment of systematic rules, comprehensive compliance guidelines and standards specifications are provided to ensure that all business units and employees can easily understand and implement data protection requirements.

ZTE has established response mechanisms such as personal data breach response, response to data subjects' right, Data Protection Impact Assessment, and other response mechanisms to effectively respond to internal and external compliance claims and risks. ZTE has incorporated compliance obligations into processes and systems to ensure the effective implementation of compliance obligations.

ZTE has established an integrated closed-loop training mechanism for curriculum development, training implementation and effect verification to promote employees' compliance awareness and improve their compliance capability in multiple dimensions. Curriculum development adopts a combination of full-staff courses, key field courses, basic publicity and implementation, and publicity and implementation of compliance in specific fields. In terms of training implementation, ZTE combines the compliance field with business fields, giving full play to the role of the full-time compliance director of each unit to achieve full coverage. In terms of effect verification, ZTE has established

an examination mechanism to promote learning, and important training is concluded by an examination to ensure the training effect.

2.1 Organizational Structure

ZTE has established a systematic privacy protection and compliance organizational structure, and formed the "three lines of defense" for compliance risk control: the Data Protection Compliance Dept., business unit compliance teams, and Compliance Audit Dept.

ZTE's Compliance Management Committee is the highest directing organization. It is responsible for the operation of the compliance management system and the decision-making of compliance affairs. Major privacy protection compliance issues are reported to the committee for guidance. The Data Protection Compliance Dept. of ZTE Corporation is a professional department that conducts privacy protection work. The department assumes responsibility for the research and adherence of global data protection laws and regulations as well as policy standards, the planning, formulation, execution and supervision of data protection compliance strategies and compliance rules. The department also assesses and reviews compliance risks in the business process.

The privacy protection teams give full play to their advantages, perform their duties, cooperate with each other, and take the risk control requirements of laws and regulations and the feasibility of policies into account to form a joint management force. The Data Protection Compliance Dept. focuses on the requirements of laws and regulations and the choice of the risk appetite. The department selects the risk appetite and establishes compliance red lines and rules in accordance with the understanding of the external legal environment and actual conditions. The BU compliance team focuses on the feasibility of compliance rules and the optimization of management costs, promotes the implementation of compliance rules, and evaluates the compliance rules. The Compliance Audit Dept. focuses on the blind spots of rules and the balance between risk control and management, inspects whether compliance risks are effectively managed, and verifies the effectiveness of the compliance system.

2.2 Management Elements

ZTE Corporation has introduced PDCA (Plan-Do-Check-Act) into the compliance business within the structure of the eight elements of the Export Compliance Program, adopting a dual-cycle model of business and management to establish the core elements of the compliance management system. The core elements are reasonable rules, comprehensive training, resolute implementation, and effective inspections. ZTE Corporation explores a risk-oriented compliance management system, taking risk identification as the orientation and using compliance management as a tool. On the basis of the construction of a top-down compliance system, ZTE Corporation enriches the content of bottom-up rules by adding scenarios and examples and promotes the in-depth integration of compliance rules and specific businesses, forming a compliance management system that fits the actual business.

In accordance with BS 10012: 2017 and ZTE's actual business situation, ZTE initially constructed the eight elements of the privacy protection management system.

2.2.1 Top management attention

ZTE Corporation attaches great importance to data protection compliance work, and the management has reached a strategic consensus that data protection compliance shall be tailored to fit the corporate development strategies. Under the leadership of the top management, the basic goals, short-term and long-term plans of the data protection compliance construction have been clarified and the benchmarking of data protection compliance work with mature industry models has been promoted to meet global customer data protection audit requirements and global regulatory agency review standards, and to prevent data protection compliance risks.

2.2.2 Governance structure

ZTE has a multi-level and professional data protection compliance coordination mechanism. We have set up a professional data protection team that includes a data protection officer, Data Protection Compliance Dept., and the BU compliance director/manager/compliance contact persons to establish, promote and implement data protection compliance management requirements. The Compliance Audit Dept. is

responsible for auditing and supervising data protection compliance work.

2.2.3 Policy and rules

ZTE has established a rule system of "policy, manuals, norm, and scenario-based guideline". We continue to promote the scenario-based and precedent-based rule system, the in-depth integration of compliance rules and specific business, and provide guidance for all departments on identifying and coping with data protection risks in business activities in accordance with the scenarios. Through the establishment of systematic rules, comprehensive compliance guidelines and standards specifications are provided to ensure that all business units and employees can easily understand and implement data protection compliance requirements.

2.2.4 Risk assessment

ZTE has refined the four dimensions of data protection compliance risk assessment, focusing on key control points for risk assessment. The four dimensions include: (1) Meeting the premises for data collection and processing; (2) Performing the duties to protect the privacy of data subjects; (3) Meeting the basic requirements of ensuring the security of user data privacy in terms of design solution selection; and (4) Ensuring the compliance of data sharing, disclosure and transmission. In terms of all business scenarios involving personal data processing, we shall meet the requirements of four dimensions of data protection compliance risk assessment, formulate specifications in accordance with roles involved in personal data processing roles, handle various risks that may exist during the processing, and instruct business units to take appropriate countermeasures.

2.2.5 Process control

ZTE has incorporated the data protection compliance requirements into various business processes to guarantee the compliance management and control points through the mechanism. ZTE has embedded the security protection of user data privacy in design into the end-to-end process of product development to ensure that the products meet the internationally accepted requirements of data protection. ZTE has established data breach response processes and data subject request procedures in IT systems to provide support and guarantee for the establishment and implementation of the compliance management process, achieving the automation

and visualization of the compliance process.

2.2.6 Supervision and inspection

ZTE Corporation has established a three-tier inspection and improvement mechanism consisting of business unit self-inspection, compliance team inspection, and compliance audit team auditing to review the violations of compliance and specify compliance risks. ZTE takes appropriate measures to prevent potential violations of compliance and establishes corresponding processing mechanisms to ensure that compliance requirements are implemented and can be modified and optimized in accordance with various business scenarios.

ZTE employees must prevent, deter and report violations. When witnessing a potential violation of data protection compliance, all ZTE employees have the right and obligation to suspend relevant business activities and to report relevant information anonymously or unanonymously. ZTE has set up multi-dimensional reporting methods including reporting to superiors, the Compliance Audit Dept., and the independent third party via email, phone or website, and hotline to encourage employees to report violations. The Compliance Audit Dept. initiates internal audit, actively investigates violations, and imposes penalties in accordance with the regulations of compliance inspection.

2.2.7 Compliance training

Compliance training is essential for raising the compliance awareness in the company and constructing a compliance culture. ZTE Corporation continues to conduct data protection compliance training, delivers clear value in various business activities, and improves and enhances employees' data protection awareness and capabilities through training, delivering the messages to all employees that compliance creates value and compliance is the cornerstone for our company's development.

2.2.8 Record keeping

ZTE maintains well-established compliance records to provide evidence of compliance and effective operation of the data protection compliance system. In addition to the data processing activities recorded in accordance with personal data record specification requirements, ZTE also keeps records on the publicity and

implementation of various data protection specifications and systematic records of data protection compliance activities.

2.3 Rule System

ZTE has established a four-tier data protection compliance system that includes the policy, manuals, norm, and scenario-based guideline.

2.3.1 Policy

Data protection compliance policy is a policy document established in accordance with ZTE's overall business policy, which specifies the red lines that should not be crossed in business activities. The establishment of the policy demonstrates ZTE's compliance with data protection laws and regulations of the country or region where the business is carried out as well as the determination of the Board of Directors and the Compliance Management Committee to give full support to data protection compliance. ZTE carries out data protection compliance work in accordance with the document.

2.3.2 Manuals

Based on the requirements of external laws and regulations, the Data Protection Compliance Manuals are general guidance documents established in accordance with compliance policies. The ZTE Data Protection Compliance Manuals consist of the Corporate-Level Manual and Manual for Business Fields, which provide basic guidance for all kinds of data processing activities carried out at the overall level and in specific business fields. The documents serve as guidance documents for all data protection compliance activities. The details are as follows:

Corporate-Level Manual: General data protection compliance policies and overall requirements are stated.

Manual for Business Fields: Based on the Corporate-Level Manual, the Manual for Business Fields further specifies the requirements by introducing business scenarios into the manual, demonstrating the compliance landscape for data protection in business fields.

2.3.3 Norm

The Data Protection Compliance Norm is the specific basis and basic support for

ZTE's data protection compliance work. Based on the mainstream laws and regulations of data protection worldwide, the Norm puts forward the basic requirements for compliance-based activities, and at the same time reserves the right to handle flexibly if the Norm needs to be adjusted in accordance with the special laws and regulations of the country or region where the business is carried out. The Norm consists of the following categories:

The management system category, which includes the regulatory document that specifies the data protection compliance management system construction; for example, the *Data Protection Compliance Regulation.*

The object definition category, which includes the regulatory documents that defines the object of data protection compliance management; for example, the *Personal Data Identification Specification.*

The general requirement category consists of the regulatory documents that specify the general requirements in the data protection compliance such as the *Rules for Judging the Foundation of Legitimacy*, the *Rules for Privacy Notification and Setting*, the *Regulations for the Administration of Personal Data Retention and Destruction*, and the *Rules for Processing Records of Personal Data*.

The special governance category, which consists of regulatory documents that specify the data protection compliance regulations for certain special circumstances; for example, the *Data Protection Impact Assessment Specification*, *Data Subject Rights Response Specification and Personal Data breach Response Specification*.

The relevant party management category, which consists of regulatory documents for the data protection compliance management of the relevant parties (customers, partners, suppliers, and etc.) involved in data processing activities; for example, the *Customer and Partner Data Protection Compliance Management Specification* and *Supplier Data Protection Compliance Management Specification.*

The data security category, which includes regulatory documents that supplement the specifications of the personal data security requirements on the basis of relevant requirements for information security; for example, the *Data Security Code*.

The compliance audit category, which includes the regulatory documents based on which the effectiveness of compliance implementation is evaluated and audited; for

example, the *Compliance Audit Management Guidelines*.

2.3.4 Scenario-based Guideline

The Scenario-based Guideline is the direct basis for the business units to carry out business activities in accordance with the compliance guidelines. As a specific guidance document, it is formed in accordance with the Norm and actual business scenarios. It specifies the data flow in the entire life cycle and the specific risks and control points in a single business activity so that the front-line employees can clearly understand the compliance requirements and the specific compliance actions, and can refer to them in the event of specific compliance problems. The Scenario-based Guideline is designed to further specify the Compliance Control Landscape. The Scenario-based Guideline is arranged in accordance with the business structure and based on the data sharing platform for collaboration, making it convenient for employees to use and make inquiries. It can also be flexibly changed as required. The Scenario-based Guideline promotes transparency and visualization of rules and ensures the timely implementation of rules.

2.4 Response Mechanism

2.4.1 Personal data breach response

We have set up a personal data breach response mechanism based on rapid multi-party cooperation, which defined our work procedures. We have specified the response procedures and managed through the "Personal Data Breach Response System" designed by experts to track and record the entire emergency response process to meet potential internal and external document retrieval and evidence submission needs. In the meantime, data emergency drills have been organized on an irregular basis to strengthen the verifiability of job responsibilities and emergency response mechanisms, avoiding data breach and handling data breach in an efficient and rational way.

In order to ensure the implementation of personal data breach policies and measures, we have set up data protection audit mechanisms and violation reporting channels. Through the work of our full-time compliance audit team, self-inspection audits have been incorporated into our internal control assurance system to perform

regular audits to promote the virtuous cycle of cultural development, resource investment, process re-engineering, and capacity improvement.

2.4.2 Personal data right response

We have set up a data subject right response mechanism based on rapid multi-party cooperation, which defined our work procedures. Data subjects can be responded to effectively when the data subjects exercise their data subject right through the Online Application Entrance. To be specific, a professional internal process response system has been built through IT-based tools, so that compliance experts and the Data Protection Officer can participate in the process and meet the requirement for quickly responding to data subjects. In the meantime, we can track and record the entire response process to meet potential internal and external document retrieval and evidence submission needs.

The data subjects can contact the Data Protection Compliance Dept. of the ZTE via the "Data Subject Right Response System" directly. At the same time, the system will ensure the security of the personal data during the process. Based on the IT-based data subject right response system, ZTE provides data subjects with high-quality interactive experience and improves social trust with good compliance behavior.

2.4.3 Data protection impact assessment

For new products, new technologies and major product service changes, to ensure that the personal data processing process meets the international data protection compliance requirements, ZTE adopts the Data Protection Impact Assessment method to carry out data protection risk assessment through IT online evaluation tools.

In actual practice, we have adopted the "Data Protection Impact Assessment" process to promote risk analysis and take related risk control measures in R&D, sales, operation, maintenance, and other main business processes. During the R&D phase, we conduct the Data Protection Impact Assessment of the personal data in order to analyze the security measures concerning permissions, logs, encryption and anonymity that have been taken to guarantee the security of personal data. Before data processing and transfer, the evaluation concerning the requirements of the relevant national laws has to be carried out. Applicable international rules must be identified and corresponding measures must be taken to lower the risks.

2.5 Risk Control

ZTE has set up a risk-oriented privacy protection compliance management system to better adapt to the changing internal and external environment, and make risk assessment an important part and a key starting point of risk management. According to the requirements of the GDPR and ISO/IEC 27701:2019, data protection compliance risk assessment covers four dimensions:

2.5.1 Meet prerequisites for data collection and processing

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

① Whether the purpose of the data processing activities has been checked and recorded;

② Whether the data processing activities have the proper legal basis;

③ Whether the consent of the data subject has been obtained and allowed to be withdrawn, and whether the acquisition of the consent is recorded;

④ Whether the required data protection impact assessment is conducted;

⑤ Whether an appropriate agreement is signed with the data processor or data controller;

⑥ Whether all the data processing activities are recorded in a timely manner.

When ZTE acts as a data processor that provides products/services to operators, the first dimension of risk assessment includes:

① Whether an appropriate agreement is signed with the data controller to clarify the relevant contents;

② Whether the personal data processing activities are carried out in strict accordance with the written instructions of the data controller;

③ Whether the relevant data obtained from the data controller will be used for marketing and advertising without the consent of the personal data subject;

④ Whether the controller is promptly notified when his/her data processing instruction violates the relevant laws and regulations;

⑤ Whether appropriate measures are taken to assist the data controller in meeting compliance requirements;

⑥ Whether all the data processing activities are recorded in a timely manner.

2.5.2 Fulfill the obligations to the data subject

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

① Whether the obligations to the data subject are clarified and recorded;

② Whether a privacy notice is provided to the personal data subject;

③ Whether there is a corresponding mechanism to realize the rights exercised by the data subject;

④ Whether there is a corresponding mechanism to respond to the requests of the data subject;

⑤ Whether the data subject is given the corresponding rights when dealing with automatic processing;

⑥ Whether the data processor who has shared the personal data or the joint data controller is notified in time when there are requests from the data subject;

⑦ Whether ZTE responds to the requests of the data subject within a specified time.

When ZTE acts as a data processor that provides products/services to operators, the second dimension of risk assessment mainly refers to whether the processor can actively assist the data controller (that is, the operators) in responding to the requests from the data subject.

2.5.3 Set the requirements of privacy by design and by default

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

① Whether personal data 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 objective of data minimization is clearly defined and recorded, or whether relevant measures will be taken to achieve the requirements for data minimization;

④ Whether the data will be deleted or demarked in time after data processing is completed; or whether the temporary documents created during the processing will

be deleted or destroyed in time;

⑤ Whether a clear personal data storage period is set;

⑥ Whether appropriate measures will be taken to ensure the safety and accuracy of data storage and transmission.

When ZTE acts as a data controller that provides products/services to the operators, the third dimension of the risk assessment includes:

① Whether the temporary documents created during the processing will be deleted or destroyed in a timely manner;

② Whether the personal data will be returned, transmitted, or disposed in a timely manner in accordance with the requirements of the agreement after the completion of the processing activities, or whether the corresponding proof will be provided to the controller;

③ Whether appropriate measures will be taken to ensure the security of data storage and transmission and that the data reaches the designated receiving location.

2.5.4 Ensure the compliance of data sharing, disclosure, and transfer

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

① Whether the basic information of the two parties, between whom the data being shared, disclosed, or transmitted, is clear, especially the jurisdiction of the two parties;

② Whether the legal basis for data sharing, disclosure, or transmission is specified, especially in cases where cross-border transfer is involved;

③ Whether the data sharing, disclosure, and transmission will be recorded in a comprehensive and timely manner.

When ZTE acts as a data controller that provides products/services to operators, the fourth dimension of the risk assessment includes:

① Whether the basic information of the two parties, between whom the data is disclosed or transmitted, is clear, especially the jurisdiction of the two parties;

② Whether the legal basis for data disclosure and transmission is specified, especially in cases where cross-border transfer is involved;

③ Whether the data controller is informed of the data disclosure requests in a

timely manner;

④ Whether the customer will be informed of the appointment and change of the personal data sub-processor in advance.

ZTE shall make a checklist of compliance control points at all levels, and ensure the effective implementation of compliance control requirements and compliance control points through activities such as self-inspections by the business units, sampling inspections by the BU compliance teams, and compliance audits and assessment. Through cyclic risk assessment and identification, the company continuously improves its compliance rules and management measures and strengthens the building of compliance.

As for the business fields, ZTE pays close attention to the changes of the business development plans and the data-related laws and regulations, constantly improves the data protection compliance rules and regulations, incorporates them into the business processes to better facilitate business development. In addition, ZTE strives to put the relevant compliance systems online so that the compliance requirements will be automatically incorporated in the business processes.

For different countries, ZTE constantly strengthens the identification and interpretation of global data compliance obligations, improves its compliance capability to support business development. In accordance with the local regulations of the key countries or regions where ZTE's business is conducted, the company provides explanation of the applicability of the rules in its data protection compliance rules system. In addition, ZTE is working on the compliance management of the local subsidiaries/representative offices in the EU/European Economic Area (EEA), and improving and updating the data protection compliance rules in accordance with the actual conditions.

2.6 Training and Capability Improvement

ZTE continuously conducts privacy protection training and publicity activities to internalize the compliance capability and promote the data protection compliance awareness of all employees. The company adopts the standardized "1+N" training mode including position-based training and scenario-based training, and uses all

kinds of new media resources such as WeChat official accounts and video courses to conduct differentiated training. In this way, the company aims to ensure that the compliance teams improve their theoretical knowledge and capability; the business unit's compliance team focuses on project progress and improves their compliance capability; the employees have the basic data protection compliance awareness; and that the personnel in key positions are clear about and fulfill their responsibilities, and provide operational guidelines for specific scenarios.

3 Promote Privacy Protection Compliance

ZTE has always been committed to achieving sustainable business development with customers, suppliers, and partners and ensuring security and compliance of the industry chain. Building privacy protection compliance together promotes partnership between the relevant parties. ZTE not only strives to build privacy protection compliance to ensure compliant operations for its products and services, but also works with partners to create a healthy compliance environment for the communications industry and widen the privacy protection ecosystem.

By embedding the concept of privacy protection by design and by default into the end-to-end product R&D process, ZTE provides customers with products that meet privacy protection requirements and prepares for markets that are increasingly concerned about privacy protection compliance. In addition, ZTE makes great effort to promote the signing of legally binding agreements, and signs the Data Processing Agreement, standard agreement terms, letter of notification, and letter of authorization with all relevant parties, to effectively control the potential risks of personal data processing. Moreover, ZTE incorporates the key control points into its business activities and processes and formulates privacy protection compliance guidelines for major exhibitions, forums, and product launches, to control privacy protection throughout the whole business process.

3.1 Compliance Creates Value

3.1.1 Fulfill corporate responsibility

ZTE is dedicated to strengthening cooperation with the supply chain in an

all-around way. We provide compliant products and services for customers or individual users and fully review the compliance capabilities of the suppliers and partners. In this way, we control risks at the source and strive to become a leading and benchmarking company in the construction of privacy protection compliance, fulfilling our corporate responsibility.

3.1.2 Foster trust in compliance construction

ZTE firmly believes that compliance creates value and upholds the idea of "Respecting Rules and Being Open-Minded." Privacy protection compliance helps the company win in the market competition, gain customer trust, and earn a good reputation. By deepening cooperation in enhancing privacy protection compliance in the industrial chain, ZTE aims to lay a solid foundation for the building of its compliance brand.

3.1.3 Ensure privacy protection of products and services

ZTE implements privacy protection by default for its products to promote privacy protection at the source and ensure compliance of its own products and services. In addition, ZTE continuously guides the relevant parties to take privacy protection by design and default as the basic element of product R&D, and promotes the industry to improve the practices and further implement privacy protection by design and default in compliance building.

3.1.4 Build a compliance ecosystem in the industry

ZTE formulates management regulations on data protection compliance for its customers, partners, and suppliers. When partnering with customers and when suppliers are introduced, the company fully evaluates and guarantees their data protection compliance capabilities by means of compliance review and agreement signing, and publicizes the importance of data protection compliance, to control risks at the source and build a data protection compliance ecosystem with all parties.

3.2 Promote Compliance with Customers

ZTE always puts customers first when providing products and services and strictly complies with commercial standards and customer requirements. According to ZTE's Data Protection Compliance Policy, the personal data involved in the products and

services provided to the customers will not be handled without the customers' authorization. Moreover, the company also provides various privacy protection designs for customers to meet users' needs and compliance requirements.

A healthy privacy protection compliance environment requires joint efforts. To remove loopholes in compliance management, it is necessary to specify the personal data involved and each party's responsibilities and obligations to data subjects, thereby forming a complete compliance chain and ensuring that all risks are under control and that the personal data is well protected.

When acting as a data processor, ZTE follows the international standards applicable to a data processor. Based on the personal data processing agreement, ZTE assists the customers in fulfilling their obligations and processes the personal data on behalf of the customers only for purposes as specified by the customers in written form. Without the consent of the data subject, ZTE will not use the personal data for marketing or advertising purposes. ZTE provides customers with appropriate information so that the customers can prove that they meet their own compliance requirements, and keeps such records to prove that ZTE fulfills its obligations to handle personal data on behalf of customers. If ZTE finds out that the instructions violate applicable laws or regulations, the customer will be notified.

ZTE assists customers in meeting their obligations to the data subject; deletes the temporary documents resulting from personal data processing within the specified period in accordance with the recorded procedure; returns, transmits, and disposes the relevant data in a safe and timely manner; informs the customers of the corresponding regulations; and ensures that the personal data is transmitted through a data transmission network under appropriate control so that the data is transmitted to the designated recipient without being leaked.

ZTE informs customers of the personal data transmission details, including the transmission to the supplier, other subjects, countries, or international organizations. The company promptly notifies customers of the basis for personal data sharing, transmission, and disclosure, as well as any relevant changes in purpose, in case the customers may object to such changes or terminate the agreement. ZTE also clarifies and records the countries or international organizations to which the personal data

may be transferred and provides customers with a list of these countries and organizations as well as the countries to which the personal data may be transferred when a sub-processor is involved. In addition, ZTE records relevant information of the disclosure of personal data to third parties, including the type of personal data, the recipient, and the time of disclosure. The disclosure of personal data includes data generated in normal operations and data required in the legal investigations or external audits. Unless otherwise provided by law, ZTE promptly notifies the customer if data disclosure is required to meet the statutory requirements and refuse any non-statutory disclosure requirements. ZTE consults the customers before disclosing any personal data or accepting any disclosure requests agreed in contracts or authorized by customers. Before introducing any sub-processors, ZTE discloses all the sub-processors to the customers and strictly complies with the agreement signed with the customers. After obtaining the general written authorization, ZTE informs the customers of any intention to add or replace the sub-processors, thereby giving the customers the right to object to such changes.

3.3 Promote Compliance with Suppliers

ZTE, as a world-renowned international provider of communications products, has partnered with a large number of suppliers, including service providers and cloud platform vendors which handle huge amounts of data. Promoting compliance with suppliers is not only an important means to guarantee the data protection compliance of ZTE, but also of great significance to the construction of a privacy protection compliance ecosystem.

ZTE has set up a privacy protection compliance framework based on the applicable laws and regulations, given priority to incorporate data protection compliance training, regulations, and processes into the supply chain, and carried out management and control of the key processes such as agreement signing and approval for cross-border data transfer, thus smoothly passing the period in which risks are not identified, and ensuring zero law enforcement, zero litigation, and zero incidents caused by public sentiment.

ZTE attaches great importance to incorporating data protection compliance requirements into the new supplier introduction process, and conducts data protection compliance control in the certification of suppliers or the procurement process. Such control measures include the signing of data protection agreements or security agreements, compliance filing, and security audits of key suppliers. Working with global suppliers and partners, ZTE looks forward to establishing a secure and sustainable commercial network that meets the data protection compliance requirements.

According to ZTE's data protection compliance requirements, suppliers shall:

(1) Strictly abide by the applicable data protection laws and regulations, and prevent any form of illegal personal data processing;

(2) Understand and comply with ZTE's Data Protection Compliance Policy, the data protection compliance terms in the contracts signed with ZTE, and other relevant agreement requirements;

(3) Support ZTE's risk management of data protection compliance and cooperate with ZTE to fulfill its data protection compliance obligations;

(4) Actively participate in the data protection compliance training organized by ZTE, and work with ZTE to establish an effective data protection compliance communication mechanism;

(5) Actively establish a complete and effective data protection compliance system, and cooperate with the data protection compliance inspections or audits initiated by ZTE;

(6) Actively take technical measures and other necessary measures to ensure data security and prevent data leakage, damage, and loss;

(7) Actively disclose or report data protection violations to ZTE.

To ensure that suppliers involved in personal data processing have due data protection and data processing capabilities and handle personal data in accordance with the laws and regulations in business activities, the following actions shall be taken to facilitate the implementation of the data protection compliance requirements for suppliers:

(1) ZTE shall conduct management and control in the certification of the supplier, review the supplier's data protection compliance capability, and draw up appropriate agreements or terms according to the products or services provided by the supplier, specifying the supplier's obligations when the personal data subject exercises his/her rights and when data leakage occurs.

(2) Due to various business scenarios, ZTE and its suppliers also have different roles in data processing activities. Usually a supplier will participate in data processing as a processor or a sub-processor. In cases where ZTE is the data controller and the supplier is the data processor, the supplier shall carry out data processing in strict accordance with ZTE's instructions. In cases where ZTE is the data processor and the supplier is the sub-processor, the customer is the data controller. As a data processor, ZTE shall meet the relevant compliance requirements of the customer and ensure that the supplier, who is the sub-processor, fulfills the compliance obligations specified by laws and regulations and the compliance requirements of the data controller. In case of personal data sharing, entrustment, and transfer with suppliers, a data protection impact assessment shall be performed and appropriate control measures shall be taken according to the evaluation results.

3.4 Promote Compliance with Partners

ZTE continuously evaluates the data protection compliance capabilities of partners in business activities based on specific scenarios and works with them to improve their capabilities and ensure that the personal data processing activities are legal and compliant.

In the Data Processing Agreement, ZTE and its partner clarify their respective roles and responsibilities of data protection and obligations when the personal data subject exercises his/her rights and when data leakage occurs. When ZTE processes personal data based on a purpose common to that of its partner, ZTE and its partner are joint data controller. In order to ensure transparent data processing, ZTE works with its partners to set due privacy notification for the data subject. When ZTE processes personal data based on a purpose different from that of its partner, ZTE and its partner are separate data controllers and set due privacy notification for the data subject

respectively.

When sharing and transferring data with partners, ZTE carries out a data protection impact assessment, and conducts data protection compliance management and signs the Data Processing Agreement when necessary. In the process of sharing and transferring the data to the partners, ZTE strictly complies with the data protection compliance requirements and the obligations specified in the agreement and keeps the relevant records. In terms of data protection compliance management, ZTE actively improves data management, reduces compliance risks, and maintains good relationships with its business partners. Regarding data processing transparency, ZTE strives to reach a balance between individual rights protection and business operations and manages to satisfy the data subjects' requests.

3.5 Promote Compliance in the Industry

ZTE continuously studies technologies and methods of privacy protection. By developing and introducing advanced privacy protection concepts and methods, ZTE comprehensively enhances its capabilities in the privacy protection of products and services to meet the privacy protection requirements of new technologies, new applications, and new modes. Adhering to the concept of Transparency, Openness, Trust, and Cooperation, ZTE works more closely with customers, partners, suppliers and standards organizations to promote end-to-end privacy protection practices and to continuously foster a secure and trusted privacy protection environment.

ZTE also actively participates in various professional meetings to share the data protection compliance ideas and practical experience. Regarding industry partners, ZTE actively shares its compliance practices and exchanges with the China Mobile Research Institute, China Mobile Guangdong, and China Mobile Jiangxi on the common issues related to data protection compliance of enterprises, such as construction of a data protection compliance system, cross-border data transfer, and interpretation and discussion of the *Cybersecurity Review Measures*. As for the cooperation with institutions, ZTE partners with various institutions and organizations, such as the British Standards Institution, DataLaws, Benchmark Chambers International & Benchmark International Mediation Center, Shanghai Academy of Social Sciences,

Shanghai Industrial Technology Institute, Shanghai Jiao Tong University, South China University of Technology, Central University of Finance and Economics, Zhongnan University of Economics and Law, and East China University of Political Science and Law. ZTE has thorough discussions with the compliance experts of these organizations on the trends of legislation and law enforcement, data protection compliance from a company's perspective, and compliance issues such as cross-border data transfer, aiming to provide professional interpretation and further explore the fields of data protection compliance.

ZTE also partners with DataLaws to hold the "5.25 Annual Meeting on Data Compliance," inviting experts from enterprises, law firms, institutions, and universities to communicate and share the data protection compliance situation and practices. In addition, ZTE also publishes the annual *GDPR Law Enforcement Case White Paper*, which provides guidance on compliance management for the industry. The Data Protection Compliance Team of ZTE has won the "Excellent Legal Compliance Team of Management Innovation" award from the CACC and the China Centre for Promotion of SME Development, and the "Privacy Strategy Contribution Award" from the BSI. ZTE is committed to work closely together with all sectors of the industry with an open, sharing, and inclusive attitude to build the privacy protection ecosystem.

4 Practice of Privacy Protection Compliance

4.1 Research and Application of Standards

ZTE attaches great importance to the research and application of standards, thus actively joins various industry associations and standards organizations, tracks policies and standards, participates in the research and formulation of standards, obtains qualification certification, and continuously studies and explores standards. Based on its data protection compliance strategy, ZTE focuses on business development and the construction of an ecosystem, promotes the application of standards by means of a suitability evaluation and continuous improvement, and improves the data protection compliance system to guarantee the development of the company.

In addition, ZTE has joined standardization associations (such as the National

Information Security Standardization Technology Committee, China Communications Standards Association, and China Electronics Standardization Association) and industry associations (such as the International Association of Privacy Professionals (IAPP), Personal Information Protection Committee of the Internet Society of China (ISC), and China Mobile Application Security Committee) and actively participated in the preparation and revision of standards.

4.2 Focus on Frontiers of Law

In terms of international operations, ZTE has paid close attention to the EU laws and regulations and guidelines issued by the European Data Protection Board (EDPB) and the data protection agencies of the EU Member States, focusing on the territorial scope of the GDPR, certification and certification criteria under Articles 42 and 43 of the GDPR, the code of conduct and supervision, the exceptional cases of data processing and cross-border data transfer necessary for the performance of a contract, to assess the impact on business. In addition, ZTE has paid attention to the international law enforcement cases, tracked and analyzed the cases, and abstracted the enforcement basis and penalty amount from the cases, thereby working out the annual *GDPR Law Enforcement Case Selection White Paper* and the *GDPR Law Enforcement Case White Paper*. Based on the cases, the company outputs scenario-based red lines and clearly determines the law enforcement focus and the risk preference.

In terms of operations in China, ZTE studies network operators' institutional management requirements for network operations security and network information security based on the *Cybersecurity Law of the People's Republic of China*. By referring to the national standards formulated and released by the National Information Security Standardization Technical Committee and the *Information Security Technology — Personal Information Security Specification (GB/T 35273)*, ZTE standardizes the behaviors of personal information controllers in information processing, including the collection, storage, use, sharing, transfer, and disclosure of information, incorporates these standards into its internal management regulations, and keeps tracking the legislation research. In October 2020, China's *Personal*

Information Protection Law (Draft) was published. ZTE actively responded to the call of the national legislature and submitted a proposal for the draft. ZTE made this proposal based on its practices in different scenarios in accordance with the international and Chinese compliance requirements, providing intelligence support for the personal information protection legislation in China from such aspects as the processing principles, cross-border transfer, and legal liability of personal information.

ZTE integrates the Chinese and international legislation and enforcement trends to form the internal resource base for legal research, including modules such as the global data protection legislation overview, lists of global data protection supervisory authorities, law enforcement case study, and global personal data protection trend tracking. In addition, ZTE interprets the key and hotly debated Chinese and international law enforcement cases and publicizes them among business units, to improve their compliance awareness and capabilities.

4.3 Privacy Protection Design

ZTE incorporates privacy by default into its products and service solutions by formulating regulations based on the concepts of privacy by design and privacy by default, specifying the principles, policies, and basic requirements for privacy protection in the product R&D process and business activities. The company also implements privacy by design throughout the entire product R&D process:

Requirement analysis phase: Identify the personal data that the products may involve, assess the personal data protection requirements, analyze whether the product functions related to personal data processing are necessary based on risk assessment and the specified personal data protection requirements and principles; and for functions to be preserved, identify the potential risks and set protection strategies based on the personal data protection requirements.

Product design phase: Design a reasonable security structure and technical measures according to the identified personal data protection requirements, review the product design plan, output data protection impact assessment reports, adjust the requirements or take targeted organizational and technical measures to address the identified risks, include personal data protection contents in the product design plan,

and keep documents related to privacy protection design to provide proof for product improvement, evaluation, management, and maintenance.

Product development phase: Implement personal data protection requirements and design, and evaluate whether the collection, use, transmission, storage, and deletion of personal data meet the design requirements when the functions are implemented.

Testing and verification phase: Verify the personal data protection measures, include the personal data protection contents in the product test scheme, and perform compliance tests.

Release phase: Conduct data protection impact assessment or review key control points before releasing a product, and organize the assessment. Only after the assessment is passed, can the product be released or deployed.

Operation and maintenance phase: Ensure that the product operation, use, maintenance, and management processes comply with the management requirements of personal data protection.

4.4 Promote Good Practices

In view of the newly promulgated laws and regulations on data protection and the lack of mature schemes and cases in the industry, ZTE has formulated the strategy of "speeding up the incorporation of compliance into business based on research, deepening the understanding of compliance based on exploration, and promoting the implementation of compliance through practices." By incorporating compliance into business, ZTE strives to strengthen awareness and accumulate experience in its practices, and cope with the challenges of risk assessment and management.

After collecting and sorting out the good practices of data protection implemented by each business unit, ZTE classifies the cases into different categories: organizational measures, technical measures, and compliance control measures, to formulate a case library of good practices of data protection. Through the presentation of the cases, the company aims to promote communication and learning of methods and practices of compliance in various business units, so that they can better understand the data protection rules and principles.

ZTE has brought forth a great deal of good practices in personal information protection, put the abstract rules into practice and refined the rules, and contributed new perspectives and experience, thus improving its capabilities and level of data protection and laying a solid foundation for further development.

4.5 Experience and Results Sharing

ZTE has been committed to sharing its experience and results, working together with partners to build systems, exchanging the resources for understanding and fulfilling obligations, and promoting communication and cooperation. Through forums and salons, ZTE keeps pace with the legislative trends, shares compliance practices and experience with its partners to grow together, and build a compliance brand together to enhance international competitiveness. Through self-media and various compliance forums and salons with professional institutions, colleges and universities, and enterprises, ZTE actively communicates with professionals in the industry to learn to cope with the difficulties of compliance more flexibly, adapt to the regulatory environment, and jointly build a sound compliance environment.

In its WeChat official account "WeAreCompliance", ZTE sets up the "Data Protection Frontiers" column to share privacy protection-related issues and updates on data protection compliance, create a convenient national legal research platform, analyze pain points in compliance control of the industry, and share practical data protection compliance practices. Moreover, ZTE publishes a series of articles, such as *Compliance With Biometrics*, *Privacy Protection Compliance Issues During the Pandemic*, and *Supervision and Enforcement Monitoring in the European Economic Area*, building up a powerful brand of privacy protection compliance.

4.6 Certification of Core Products

ZTE takes security as the highest priority in product R&D and service delivery activities and is committed to providing reliable, end-to-end, full lifecycle security assurance. Since 2005, ZTE has passed the certification of the ISO/IEC 27001 Information Security Management System, which is updated annually and covers all ZTE's services.

In 2020, ZTE introduced and established the Personal Information Management System (PIMS) for the core product line in accordance with the international standard ISO/IEC 27701: 2019 Privacy Information Management System and the best practices in the industry, and continuously improved the system based on its actual practices. At present, the key 5G products selected by ZTE has passed the ISO/IEC 27701 certification and obtained the certification certificate. In addition, ZTE has made continuous effort to study the authoritative privacy authentication mechanism in the industry, improve the privacy protection system, to build a sustainable, transparent, open, and sound privacy protection environment.

5 Major Events

- Won the Privacy Strategy Contribution Award by BSI, December 2020
- Published the *Good Practice of ZTE Data Protection Compliance (2020)*, December 2020
- Incorporated the principles of privacy by default into the R&D process, December 2020
- Incorporated the principles of privacy by default into the terminal R&D baseline, October 2020
- Formulated the ZTE Data Protection Compliance Control Landscape, July 2020
- Obtained the certification of the ISO/IEC 27701: 2019 Privacy Information Management System, May 2020
- Held the 5.25 Annual Meeting on Data Compliance (2020), May 2020
- Published the *5G Application Scenarios and Privacy Protection Research Report,* May 2020
- Published the *GDPR Law Enforcement Case White Paper (2020),* May 2020
- Published the *ZTE Privacy Protection White Paper (For Internal Publicity),* May 2020
- Published the *Global Privacy Compliance Policy Guide on Epidemic Prevention,* May 2020
- Published the *Good Practice of ZTE Data Protection Compliance (2019),* December 2019

- Won the Excellent Legal Compliance Team of Management Innovation Award from CACC, November 2019
- The Data Subject Rights Response System (DSRRS) went online, November 2019
- Published the *GDPR Law Enforcement Case Selection White Paper (2019),* October 2019
- Established the Data Leakage and Emergency Response Simulation Exercise Mechanism, July 2019
- Held the "China Data Compliance Salon • Shenzhen Station", April 2019
- The Data Breach Incident Management System (DBIMS) went online, April 2019
- Put the operator GDPR compliance management system, ZXRDC into operation, March 2019

Concluding Remarks

Compliance safeguards operations, compliance creates value. ZTE always regards compliance as the cornerstone of its strategy and the premise and bottom line of its operation. Under the guidance of the overall compliance values, ZTE strives to promote the construction of privacy protection compliance, further identify the global data protection compliance obligations and incorporate them into our internal regulations, improve the data protection policies, regulations, guidelines, and processes in accordance with the mature models in the industry. With these efforts, ZTE aims to meet the requirements of data protection audits of global customers and the review standards of global supervisory authorities, and prevent global systematic data protection compliance risks.

ZTE has established a complete compliance system and implemented systematic risk control. For ZTE, privacy protection is not only a legal requirement, but also the building block of trustworthy and ethical business conduct. Compliance is not a slogan, but a social responsibility of the company and the responsibility of every ZTE employee. All ZTE employees shall remain true to the original aspiration, adhere to compliant operations, safeguard value and create value, foster the spirit of striving for innovation and progress, to guarantee steady development, and establish a strong compliance brand. Let's create value and share a better future!

ZTE Privacy Protection White Paper

Comply with Laws | Build Trust Together | Value Business Ethics

By Yang Yuxin, Chen Piaopiao, Song Weiqiang, Mao Anna, Peng Huanhua, Wang Zhiyu, Gao Ruixin, Zhang Han