ZTE Privacy Protection White Paper

COMPLY WITH LAWS | BUILD TRUST TOGETHER | VALUE BUSINESS ETHICS

2022

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 and adjustment of products or services, continuous optimization of the compliance system, or other reasons, ZTE has the right to add, modify, delete, and invalidate the content of this document, or update it occasionally. 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 been providing innovative technologies and integrated solutions for global operators, enterprise customers, and consumers across the world.

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

Attaching great importance to **privacy protection**[1], ZTE 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 effective supervision and advanced tools, and incorporated the system into business processes, to continuously improve its privacy protection capabilities and fully meet the relevant requirements.

ZTE incorporates privacy protection into the process 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 compliantly.

ZTE actively exchanges with industry partners, and makes proactive efforts, including holding forums, releasing achievements, providing suggestions, and participating in the 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 (2022)

1 Privacy Protection Policy

With the development of the digital economy, privacy protection has been a popular topic widely discussed by the public, consumers, legislatures, and supervisory authorities, and privacy compliance thus has become a focus of various industries. As a multinational ICT company, ZTE 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" in line with the company's compliance objectives.

1.1 Vision for Compliance

Build a scientific, applicable, and effective privacy protection compliance system.

ZTE strives to build and continuously improve a privacy protection compliance system which complies with laws and regulations, meets the requirements of supervisory authorities, applies to the industry characteristics and the company's business activities, and is fully integrated with the company's governance system. Specifically, the rules in the system are easy to access, understand, and follow, and are effectively publicized and continuously improved. The compliance requirements are incorporated into the business processes, and implemented under strong supervision based on business scenarios.

ZTE also strives to improve the effectiveness and efficiency of privacy protection. The company makes complicated compliance requirements easy to understand, to promote their effective implementation. To improve the efficiency of privacy protection, ZTE sets key control points for main business and key products, develops IT systems to reduce manual controls and offline operations, and achieves a balance between compliance costs and management resources investment. Through all these efforts, ZTE aims to be a pioneer of privacy protection in China and to proactively practice privacy protection across the world.

1.2 Mission for Compliance

Ensure that the privacy protection compliance system supports risk control, trust enhancement, and brand building.

ZTE continuously promotes the concept of "Compliance Creates Value" and takes actions accordingly. The company carries out compliance work in strict accordance with laws and regulations, and incorporates compliance requirements into business activities to win customers' trust and build a compliance brand. In addition, ZTE earnestly explores innovative compliance solutions while actively learning from first-class compliance practices. Based on its global risk management and control, ZTE makes great efforts to turn compliance investment into customers' trust in its products and services.

ZTE continuously integrates the risk control, trust enhancement, and brand building for privacy protection. In terms of risk control, the company complies with applicable laws and fulfills its obligations to eliminate potential risks and reduce violations. Facing risk events, ZTE responds to them 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 win the trust of multiple parties. Regarding brand building, ZTE respects digital and privacy ethics, and puts emphasis on the privacy protection of users, customers, and employees in corporate values, improving their recognition in ZTE's privacy protection efforts and enriching the corporate brand.

1.3 Compliance Objective

1.3.1 Compliance with Legal Requirements and Risk Prevention and Control

ZTE complies with the applicable privacy protection laws and regulations in the countries/regions where it conducts business. The company continues to identify external privacy protection obligations and transform them into internal rules, improve internal policies, regulations, guidelines, and processes, and learn 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 respects the privacy concerns of users and all stakeholders, and protects their privacy rights. The company continues to promote the effective implementation of compliance requirements in business activities, and integrate compliance management with business practices. Through reasonable rules, comprehensive training, and effective implementation and supervision, ZTE ensures that all employees respect rules and external parties trust the company in its compliance work.

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 customers, partners, suppliers, shareholders, and employees through its 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 by incorporating it into the company's compliance strategy, and regarding privacy protection compliance as one of the three key fields of compliance, to ensure the effective implementation of compliance requirements in business activities. With the tone from the top, ZTE continues to invest resources in its regulations, processes, mechanisms, management, technologies, and tools, and introduce services from law firms and consulting institutions, to accumulate compliance knowledge and experience and strengthen capabilities.

1.4.2 Well-Structured System and Capability Development

ZTE has established a compliance management system 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 compliance requirements and strict implementation of regulations and processes through continuous compliance training and compliance capability development. The purposes are to guide the fulfillment of compliance requirements, provide timely compliance consulting, and effectively implement measures for compliance.

1.4.3 Integration of Compliance into Business and Creation of a Sound Environment for Compliance

ZTE has created a good environment for compliance, in which the Data Protection Compliance Dept. builds the privacy protection compliance system, business units stick to compliance requirements, and all employees participate in compliance work. Specifically, the Data Protection Compliance Dept. formulates relevant compliance policies, manuals, and guidelines, optimizes management and control processes, and promotes the incorporation of compliance into business. Business units strictly implement compliance requirements, and fully disclose, continuously reduce, and jointly handle various risks. All employees respect the rules, take the initiative to provide suggestions, and participate in the building of a compliance management system.

1.4.4 Reconstruction of IT Systems and Introduction of Tools

ZTE actively adopts applicable technologies and measures for privacy protection, and promotes the digital transformation of compliance management through the reconstruction of IT systems, introduction of professional tools, and improvement of technical solutions. By incorporating the tools and solutions into the existing management processes and IT systems, the company ensures that all procedures of data processing can be recorded, queried, traced, and verified, thus achieving comprehensive, integrated, and automatic management and control.

2 Privacy Protection Framework

ZTE has established company-level privacy protection rules that comply 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. ZTE implements special governance for key business and countries, and incorporates privacy protection requirements into product design, service delivery, and internal control and management to promote the integration of compliance management with business, and support product innovation with compliance.

To build a risk-oriented compliance management system for privacy protection, ZTE not only performs compliance management in a top-down manner, but also incorporates scenario-based compliance rules into business activities to match the actual business.

With great importance attached to privacy protection from the management, ZTE has aligned privacy protection compliance with its corporate development strategy, and specified the objectives and long-term planning of privacy protection compliance management. By learning from first-class cases and experience in the industry, ZTE has not only effectively prevented privacy protection risks, but also met the expectations and requirements of stakeholders.

2.1 Organizational Structure

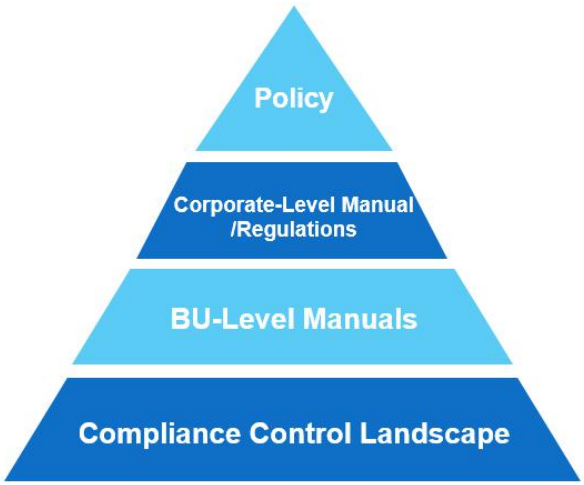
ZTE has established a collaborative working mechanism for privacy protection compliance. Under the Compliance Management Committee, the privacy protection team is composed of the Data Protection Officers (DPOs), the Data Protection Compliance Dept., and BU compliance directors/compliance managers/compliance contact persons. The team is responsible for formulating and implementing compliance management requirements. 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 compliance matters of data protection and providing guidance accordingly. As a specialized department for privacy protection, the Data Protection Compliance Dept. is responsible for researching and interpreting global data protection laws and regulations, policies, and standards, and planning, formulating, implementing, and supervising privacy protection compliance strategies and rules, and assessing and inspecting compliance risks in specific business processes.

ZTE implements privacy protection based on the collaboration of the Data Protection Compliance Dept., BU compliance teams, and the Compliance Audit Dept. The Data Protection Compliance Dept. formulates compliance rules based on the legal requirements and the company's risk appetite. BU compliance teams promote the implementation of compliance rules, and evaluate the necessity and reasonableness of the rules to optimize OPEX. 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 punishing violators accordingly.

2.2 Rule System

ZTE has established the data protection compliance rule system, which consists of the compliance policy, *ZTE Compliance Manuals for Data Protection - Corporate-Level Manual*/regulations, BU-level manuals, and Compliance Control Landscape.



2.2.1 Policy

The compliance policy refers to a series of documents established in accordance with ZTE's overall business policy, which specifies the red lines that shall never be crossed in

business activities. The establishment of the policy demonstrates ZTE's compliance with data protection laws and regulations, and the determination of the Board of Directors and the Compliance Management Committee to fully support data protection compliance. The policy serves as a guidance for ZTE to carry out data protection compliance.

2.2.2 Corporate-Level Manual/Regulations

The compliance manuals are formulated to provide general guidance for compliance work based on external laws and regulations and ZTE's compliance policy. The *Corporate-Level Manual* 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 are detailed requirements of key control points, or the requirements formulated separately to adapt to the ever-changing external laws and regulations by specifying the key obligations and compliance requirements of the laws and regulations.

2.2.3 BU-Level Manuals and Compliance Control Landscape

The BU-level manuals refer to the specific requirements formulated based on the characteristics of each business field and the *Corporate-Level Manual*.

The Compliance Control Landscape involves scenario-based requirements to jointly provide privacy protection compliance guidance for business fields with the BU-level manuals. Developed based on the business structure, the Compliance Control Landscape has been launched on the digitalized collaboration platform for the easy access by employees and update based on the requirements, thus ensuring transparent and timely implementation of the compliance rules.

2.3 Process Mechanism

ZTE develops IT systems for its key obligations such as data breach response, response to Data Subject Right (DSR) requests, and Data Protection Impact Assessment (DPIA), and incorporates the systems into business processes to facilitate cross-departmental collaboration and automatically keep operation records that can prove the effectiveness of the compliance system.

2.3.1 Personal Data Breach Response

ZTE ensures that its personal data processing activities comply with laws and regulations by improving its management regulations, strengthening training, and organizing emergency drills, to reduce the probability of personal data breaches. In case of actual, suspected, or potential personal data breach events, the Personal Data Breach Response System will be applied to implement the response process (including reporting, judgment, analysis, handling, repair, notification, review, and improvement) and automatically record relevant operations to meet such requirements as multi-party collaboration, retrieval of internal documents, and submission of evidence to external parties, thus handling personal data breaches in a more scientific and proper manner.

2.3.2 Response to DSR Requests

ZTE has provided IT-based, easy-to-use, and open channels for data subjects to apply for exercising their rights, thus ensuring that DSR requests are promptly accepted and

comprehensively managed. With the collaboration of privacy compliance experts, the DPOs, business leaders, and technical engineers in the response process, ZTE responds to data subjects in a professional, objective, and appropriate manner. The whole response process will be automatically tracked and response records generated. In this way, ZTE provides good interactive experience for data subjects to demonstrate its commitment to privacy and enhance the public's trust.

2.3.3 DPIA

ZTE uses the DPIA System to evaluate new products, new technologies, and major changes in products and services online, thus ensuring the compliance of personal data processing activities that have a significant impact on individual rights and interests. In the R&D phase, ZTE assesses the types of collected personal data and analyzes the privacy protection measures taken for permissions, logs, encryption, anonymity, etc. Before processing and transferring personal data, ZTE checks whether relevant compliance requirements are met and takes corresponding compliance measures to reduce business risks.

2.4 Risk Management and 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 controller 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 data 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 data processor or other data controller involved.

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

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

(1) Whether an appropriate agreement is signed with the data controller to specify 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 is used for marketing and advertising with the consent of the personal data subject.

(4) Whether the data controller is promptly notified when its data processing instructions violate 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 comprehensive and timely manner.

2.4.2 Obligations to Data Subjects

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

(1) Whether the obligations to the data subject are specified 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 automated processing is involved.

(6) Whether the data processor who has shared the personal data or other data controller involved is notified in a timely manner when there are requests from the data subject.

(7) Whether the requests of the data subject are responded to within a specified time.

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

2.4.3 Privacy by Design (PbD) and Privacy by Default

When ZTE acts as a data controller that provides products/services directly to individual users, the 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 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 de-identified in a timely manner after data processing is completed; or whether the temporary documents generated during the processing is deleted or destroyed in a timely manner.

(5) Whether a clear personal data 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 a 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 data 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 to the data controller.

(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 controller that provides products/services directly to individual users, the risk assessment includes:

(1) Whether the basic information of 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 a data processor that provides products/services to customers and partners, the risk assessment includes:

(1) Whether the basic information of 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 controller is informed of the data disclosure requests in a timely manner.

(4) Whether the customer is informed of the appointment and change of the personal data sub-processor 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 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, in improving 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 a focus on 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 is actively promoting the co-building of privacy protection with industry partners. To be specific, the company takes privacy protection as a consensus to be reached 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 security-related departments play an important role in internal co-building. ZTE has established a collaborative working mechanism for data security and compliance, gathering experts in 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 scenarios of privacy protection such as cross-border transfer of

personal data and the use 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, engineering services, event management, and various functional fields, thus forming a system that guarantees cybersecurity throughout the product lifecycle. The *ZTE Cybersecurity White Paper - Providing Customers with Secure and Trustworthy Products and Services* systematically introduces how ZTE implements cybersecurity governance and the PbD approach throughout the product lifecycle by following industry standards and best practices.

Adhering to the principle of openness and transparency, ZTE has established cybersecurity labs in China and Italy as well as transparency centers in Belgium and Turkey, 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 sets up a security reward program to continuously encourage feedback from security practitioners and institutions worldwide on security issues found in products and services.

Cybersecurity is closely related to privacy protection. In overseas markets, especially the European market, supervisory requirements for cybersecurity and privacy protection are continuously strengthened, and customer requirements are becoming stricter. In the whole process of product delivery, ZTE implements systematic management and technical specifications for 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 supervisory authorities, participating in industry conferences and forums, and publicizing the company's security measures and achievements.

3.1.2 Information Co-Management

ZTE implements information management and control across the lifecycle to guarantee the confidentiality, integrity, and availability of information. With an integrated information security management system, and archives and document management system, ZTE conducts regular security inspections, and identifies and investigates the violations to improve the information management awareness of all employees.

ZTE has launched a project to strengthen personal information security governance and to reduce risks of personal data breaches and abuse. The project aims to: 1) Identify the high-risk systems containing personal data, and include the exporting of personal data on the back end of the high-risk systems into the scope of the internal information security audit; 2) Determine whether to include the systems that contain personal data as identified and reported by the business units in the follow-up governance, and; 3) Incorporate the security governance requirements of "data display, export, and exchange" into the process and ensure the system functions that do not meet the requirements are not launched. Under the

project, 100% data de-identification governance is achieved in the high-risk systems, and the personal data of the company's employees, customers, and partners is protected in accordance with the requirements of laws and regulations, demonstrating that ZTE has practiced the philosophy of privacy protection and compliance, obtained internal and external trust, and conducted proactive actions on compliance to deeply integrated the 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 the information system, and may infringe on the rights and interests of data 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 business standards and customer requirements, ZTE aims to achieve comprehensive personal data protection. ZTE and its customers identify their respective responsibilities and obligations in the commercial agreement to maintain a healthy privacy protection environment together.

When acting as a data processor, ZTE follows the applicable international standards. Based on the *Data Processing Agreement* (DPA), ZTE assists the customers in fulfilling their obligations and processes the personal data on behalf of the customers only for the purposes as specified by the customers in written form. Meanwhile, ZTE provides customers with appropriate information so that the customers can prove that they meet their own compliance requirements, and keeps the aforementioned records necessary to prove that ZTE fulfills its obligations to process personal data on behalf of the customers. Moreover, ZTE assists customers in meeting their obligations to the data subjects. For example, ZTE deletes the temporary documents generated during personal data processing within the specified recording period, returns, transfers, and disposes of the relevant data in a safe and timely manner, and provides the management system for the customers, to ensure that the personal data is transferred through a data transfer network under appropriate control and the data is transferred to the designated recipient without being breached.

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, to develop a privacy protection compliance ecosystem together with the upstream and downstream of the supply chain.

ZTE implements compliance controls through key control points, including signing agreements with suppliers and approving data cross-border transfer. In the supplier introduction and certification phase, ZTE reviews the suppliers' data protection compliance capability, and drafts appropriate agreements or clauses in accordance with the products or services provided by the suppliers, including data protection agreements or security agreements, compliance recordkeeping, and security audit on key suppliers. Such agreements or clauses clearly stipulate assistance obligations of suppliers in the cases of the exercise of DSRs or personal data breach. For different business scenarios, ZTE distinguishes between "controller and processor" or "processor and sub-processor" in data

processing activities to fulfill the corresponding compliance obligations stipulated by laws and regulations. If there are cooperation relationships such as personal data sharing, entrusted processing, and transfer between ZTE and the suppliers, the DPIA shall be performed according to the specific situation, and the corresponding management and control measures shall be taken according to the assessment results.

3.4 Co-Building with Partners

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

In the DPA, ZTE and its partners specify their respective roles and responsibilities of data protection, and obligations to be fulfilled when the data subjects exercise their rights or data breaches occur. When ZTE and its partner process personal data for the same purpose, ZTE and its partner are joint data controllers. In order to ensure transparent data processing, ZTE works with its partners to provide due privacy notice for the data subjects. When ZTE and its partner process personal data for different purposes, ZTE and its partner are separate data controllers who provide due privacy notices for the data subject respectively. When sharing data with or transferring data to its partners, ZTE strictly complies with the data protection compliance requirements and the obligations specified in the agreement.

3.5 Co-Building with Industries

Adhering to the philosophy of transparency, openness, trust, and cooperation, ZTE keeps abreast of advanced technologies and methods of privacy protection through exchanges within industries, and comprehensively enhances its privacy protection capabilities to meet the compliance requirements under new technologies, new applications, and new business.

ZTE keeps exchanging with supervisory authorities, industry organizations, technical institutions, and colleges and universities about the interpretation of the latest laws, compliance system building, and cross-border data transfer for effective implementation of compliance requirements. In March 2021, ZTE hosted the 2nd Multinational Corporation Trade Compliance Symposium. In the sub-forums on anti-bribery, anti-money laundering, and data protection, ZTE discussed the global compliance governance of cross-border data flows and data protection compliance from the perspective of the public media, introduced the key points in data protection compliance management for multinational enterprises, and shared its own practice in data protection compliance management. In December 2021, ZTE hosted the second Legal and Compliance Scholars Forum - Seminar on Data Security and Personal Information Protection. In the seminar, renowned professors were invited to discuss the latest situation of the *Data Security Law of the People's Republic of China* and the *Personal Information Protection Law*, as well as the data security and personal information protection, which provided a reference for compliance governance to enterprises in the industry.

4 Privacy Protection Practice

4.1 Research on Laws and Regulations

ZTE pays close attention to the data protection rules in key countries and regions around the world, studying external rules and translating them into applicable internal rules. The

requirements for data collection, storage, use, sharing, transfer, and public disclosure in the following regulations are integrated into ZTE's internal rules, including:

1) Global mainstream data and privacy laws such as the GDPR;

2) *China's Cybersecurity Law*, *Data Security Law*, *Personal Information Protection Law,* and supporting documents;

3) International standards such as the ISO/IEC 27701 *Privacy Information Management System*;

4) National standards such as GB/T 35273 *Information Security Technology Personal Information Security Specification* issued by the National Information Security Standardization Technical Committee.

ZTE has established a privacy protection space with sufficient legal resources such as global data protection legislation, a list of supervisory authorities, and European law enforcement cases, which is open to business units and compliance teams for easy access at any time and capability development. The legal research results are sorted out and summarized to compile the *GDPR Law Enforcement Cases Selected White Paper* and *GDPR Law Enforcement Case White Paper*. The red lines of business activities are developed based on actual law enforcement cases, so that the focus of law enforcement can be identified in a risk-oriented manner and high-risk activities can be avoided. Based on the annual compliance governance projects, ZTE has summarized the results into professional reports including *5G Application Scenarios and Privacy Protection Research Report*, *White Paper on Data Cross-border Compliance Governance Practice*, and *Privacy by Design (PbD) Research Report*, to continuously create value and provide long-term guidance for compliance management.

4.2 Business Practice

As the laws and regulations in the field of privacy protection are frequently updated and published, and the mature management plan is relatively lagging behind, ZTE adopts the basic strategy of "transformation fueled by research, compliance understanding deepened by exploration, implementation advanced by practice" to encourage the integration of compliance requirements into business, accumulate practical experience in the various scenarios, and tackle complex and volatile challenges.

ZTE forms a set of good practice cases of privacy protection implemented by business units, involving organizational measures, technical measures, and compliance control measures. The publicity of such cases promotes the exchange and learning of the compliance methods and control measures among different business units of the company, so that the data protection compliance measures are continuously optimized.

ZTE encourages business units to implement data protection rules based on their own business characteristics, so as to generate a large number of good practices for personal information protection, accumulate practical experience, strengthen the compliance foundation in business, and eventually enhance the overall privacy protection capabilities of ZTE.

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 data processing include customer relationship establishment and maintenance, customer visits and receptions, and business exhibitions. In addition, scenarios that involve

the signing of agreements to specify data processing rights and responsibilities with customers 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 customers, such as the names, telephone numbers, and email addresses, are mainly processed for daily business communications. Privacy protection and control are implemented through the information systems to ensure that the collection, storage, and use of personal data comply with the principle of data minimization. In special cases, when a customer is invited to visit ZTE or participate in an exhibition, it is necessary to book an air ticket or hotel for the customer. If sensitive personal data such as a passport or ID number needs to be obtained, the business team will notify the customer of the purpose of collecting and processing his/her personal data in an appropriate way (such as sending a *Privacy Notice*), obtain the consent of the data subject, and delete the personal data immediately after the activity ends.

In the business scenario of bidding management, if the personal data held by the customer needs to be processed, the business team will sign the DPA with the customer to obtain the authorization for data processing. If data cross-border processing is involved, the corresponding customer authorization will also be obtained beforehand.

To provide overseas operators with technical support for fulfilling contract obligations, if it is necessary to obtain data from the customer's network and transfer such data across borders, the business team shall identify the aforementioned requirements during the contract signing review phase and inform the customer of the requirements, and fully disclose the data processing purposes, data transfer paths, data types, and technical and organizational measures for ensuring data security. Only after the customer's authorization is obtained and the internal approval process of ZTE is completed, can the cross-border operations be performed.

4.2.2 System Product

ZTE's system product business involves wireless products (RAN, core network, and server), wired products (transport network, fixed network, and multimedia products), digital energy products (energy products for communications), and the product-related solutions. The cybersecurity and data security settings of the system products will directly affect the user's personal data security. The settings focus on the PbD, realization of DSRs, product security reinforcement, and permission management.

The system product R&D team incorporates the PbD into the High Performance Product Development (HPPD) process. Through specific steps including risk identification, solution design, pilot project, and specification revision and release, the full-lifecycle risk management and control of personal data is incorporated into the R&D requirements management, system design, development verification and product launch through PbD and privacy by default. The implementation of PbD incorporated in the R&D projects will be checked and accepted during in milestones such as project technical review and version release.

The system products that have been officially launched are periodically evaluated. For example, the DPIA is required in the system solution phase of the HPPD process. The details include:

(1) Risk identification: Identify potential risks. Each department/project of System Product shall identify and record potential threats and product vulnerabilities in the full lifecycle of data processing from two aspects: DSR protection and data security

based on the identified personal data and data flow.

(2) Risk analysis: Use the *Personal Data Sorting and Data Protection Impact Assessment Tool* to analyze risks in terms of the possibility and consequences of risk occurrence.

(3) Risk evaluation: Determine the risk level of the identified risk items in accordance with the results obtained in the risk analysis phase.

(4) Risk treatment: Determine the risk treatment strategies, and formulate and implement the risk treatment plans in this phase. Optional risk treatment strategies include adopting control measures to reduce risks, and adjusting business requirements to avoid risks, transfer risks, and accept risks.

(5) Result review: Based on the data processing status, data protection compliance requirements, basic data protection principles, and data protection risk assessment, fill in the *DPIA Report Template of System Products* in a timely manner, and record data protection compliance requirements, data processing scenarios, security control measures, assessment results, treatment solutions, treatment plans, accepted and recorded risk items, and the list of unsolved problems. After the first draft of the DPIA report is formulated, submit it to the product security team for review.

(6) Report management: Archive the documents that have passed the technical review in accordance with the guide to the PbD for system product R&D.

4.2.3 Engineering Service

ZTE's engineering service refers to 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 data protection compliance include technical delivery, customer support, and engineering outsourcing management. The types of the involved data include network data of operators, network user data, and personnel information of third-party partners.

In line with the characteristics of business activities in the engineering service field, the *ZTE Data Protection Compliance Manual - Engineering Services* has been formulated. The manual specifies risk-oriented and scenario-based guidelines for data protection of engineering service activities, and business scenarios and processes into which data protection rules are incorporated to ensure that the rules are effectively implemented.

The related data protection management and control requirements are publicized to employees through data protection training, publicity activities, and data protection highlights, so that employees can better understand the necessity and details of related management and control measures, preventing ineffective implementation due to inconsistent understanding of data protection requirements.

ZTE focuses on the scenarios and processes of high-risk business activities by establishing the KCP inspection mechanism applicable to the engineering service field, and inspects and evaluates the implementation of the KCPs in the related business activities by the employees, thus ensuring the effective implementation of the KCPs. By analyzing the inspection results of KCP implementation, collecting and giving feedback on the employees' suggestions on the KCP implementation, and obtaining audit suggestions from external institutions, ZTE reviews the reasonableness of the KCPs, and optimizes the KCP setting and implementation modes in a timely manner, so as to continuously improve the effectiveness of management and controls and reduce the cost of rule implementation while ensuring that the

KCPs cover the major data protection risks in business activities.

In technical delivery activities, when providing services such as network maintenance and troubleshooting, ZTE, as a data processor, inevitably needs to process the customers' network user data, and even support from R&D experts in China is required for addressing some network problems. To meet the requirements for cross-border data transfer under the GDPR, in accordance with the manual and the characteristics of business scenarios, ZTE formulates the scenario-based guidelines as well as the data protection management and control requirements and measures for remote access services:

(1) In accordance with the GDPR, sign the DPA/Standard Contractual Clauses (SCCs) with the customer acting as a data controller, and incorporate the signing status of the relevant agreement into the business process of remote access for technical delivery. Through system control, the remote access service can be started only after the SCCs are signed.

(2) Incorporate approval requirements into the business application process, and evaluate the necessity of remote access.

(3) Use the network access solution approved by the customer and build a security house dedicated for data processing, and take organizational and technical measures to ensure the security of data processing.

(4) Incorporate the requirements for recording data processing activities comprehensively and promptly into the application process of the business system, so that the employees can record the processing activities during the application for, execution of, and closure of the remote access service.

(5) Regularly check and audit the implementation of data protection compliance management and control actions for business activities to ensure that the related requirements are implemented effectively.

4.2.4 Terminal

The terminal business of ZTE is a series of activities for the production, design, sales, and aftersales services of terminal products. The activities include product R&D, product operation, sales, product supply and customer service, brand management, and quality management.

By sticking to the privacy compliance bottom lines for terminal product management, safeguarding the company's compliance image, and creating brand value for ZTE's compliance management in the terminal field, ZTE strives to present a trustworthy terminal brand to its users and the society. ZTE has always been committed to promoting user experience in terms of ZTE's privacy protection, and has been continuously providing more secure products and services for users. The PbD concept has been incorporated into ZTE's terminal product R&D lifecycle, to ensure that with a reliable organization, process, and technical management system for privacy protection, all personal data is protected in an all-round manner and processed in accordance with compliance regulations.

To meet the supervision requirements for privacy compliance on apps, the compliance review process is formulated for external release of products and pre-installed apps. Before the external release, strict privacy compliance reviews are conducted, the problems identified during the reviews are rectified, and the compliance risk identification and control are carried out by the relevant business units, BU compliance teams, and experts from the compliance COE. As for privacy protection technologies, ZTE adopts methods such as data encryption, breach prevention, and database audit to protect consumer privacy. ZTE's AppSecScanner, a

self-developed detection tool for automatic scanning of security vulnerabilities and privacy compliance risks, enabling a closed loop from compliance reviews to technical supervision through static and dynamic scanning. For other scenarios besides product R&D, such as e-commerce, supply chain, customer service, aftersales service, survey, and crowdsourced testing, all-round processes and regulations have been formulated to ensure that all business procedures meet the data protection compliance requirements.

As the regulation on the privacy protection of apps gets tighter in China, the terminal product security team has carried out in-depth research on app security, and has independently developed and applied a detection platform, AppSecScanner, for terminal products to ensure privacy security and compliance. The R&D and launch of AppSecScanner has enabled the detection of a large amount of code, thus saving the human resources in detection and the expense of purchasing third-party detection tools, and effectively supporting the realization of detection requirements of app development units, including ZTE Mobile Device Division and System Product. This detection platform demonstrates ZTE's compliance achievements in the terminal field, including its development of compliance rules and product-based compliance management, reflecting that compliance truly creates value for the company.

4.2.5 Supply Chain

ZTE's supply chain business is the entire management process of the design, planning, control, and optimization of the material flow, information flow, and financial flow, which integrates the upstream and downstream, minimizes the internal friction, optimizes the company's overall efficiency, ensures the members in the supply chain achieve the corresponding performance and benefits, and rapidly meets the customer demands. Supply chain activities that involve personal data processing include procurement, logistics management, and reverse logistics. Scenarios involving privacy protection in procurement include supplier certification, training, and conferences; scenarios involving privacy protection in logistics management include transportation, warehousing of finished products, and customs affairs; and scenarios involving privacy protection in reverse logistics include the destruction and sale of scrapped products.

In the business activities such as procurement, logistics management, and reverse logistics, ZTE may process information such as the name, telephone number, email address of the business contact persons provided by customers and suppliers, so as to facilitate the receipt, delivery, and repair of goods. In the supplier certification scenario, the name and contact information of the senior management as well as sales and financial personnel provided by suppliers may be processed to ensure that the certification and the subsequent business negotiations, bidding, and payment are conducted smoothly. In the above scenarios related to personal data processing, ZTE strictly complies with the applicable laws and regulations on personal data processing, and effectively protects personal data. The main management and control measures include the following:

(1) Based on the requirements for transparency and privacy notices as well as a legal basis, when collecting the personal data provided by suppliers, ZTE informs the data subjects of the purpose and other necessary information of data collection and processing in a proper way (by providing the privacy statement or sending emails), and, when applicable, obtains the consent of the data subjects;

(2) Only the minimum range of personal data that is related to the business and necessary is collected;

(3) For a procurement contract signed with a supplier on the personal data provided by ZTE or ZTE's customers or other suppliers, ZTE investigates, audits, and supervises the contracted supplier's capabilities of personal data protection and signs appropriate data protection agreements (data protection clauses, DPA, Data Transfer Contract, etc.) with the contracted supplier;

(4) To guarantee the rights of data subjects, ZTE responds promptly and effectively to suppliers' or individuals' requests for access, deletion, or modification of the personal data related to supply chain business that is processed by ZTE;

(5) ZTE evaluates the personal data storage period. After the cooperation with a supplier terminates, ZTE deletes the related personal data based on the external laws and internal processes, and requires and promotes the supplier to delete the personal data in accordance with the requirements specified in laws, regulations, and the contract.

(6) When storing and transmitting the personal data provided by a supplier, ZTE implements permission management, data encryption, and retains operation logs in IT systems;

(7) For products returned by customers, ZTE assesses whether any personal data is contained in the scrapped products, and adopts appropriate physical disposal methods based on the assessment result, so as to reduce the risk of the illegal access of personal data.

Products that are returned by customers (operators) and components replaced during repair and maintenance may contain the personal data of customers (operators) or end-users. Under such situation, it is necessary to control the risk of breaches and improper processing of the data. ZTE supply chain erases or destroys data on the storage devices replaced in repair and maintenance. If physical processing is required by the recycler, the recycler is required to sign the security agreement and provide processing reports, so as to reduce the risk of personal data breaches.

4.2.6 Headquarters Functional Areas

ZTE's headquarters functional areas include the operations management of the company, the administration affairs and real estate services that support the productivity of the core business, and the public affairs related to government and industry associations or institutions, universities, and research institutes.

Since the headquarters functional areas cover a wide range of business and a large number of activities, the company mainly adopts a scenario-based approach to manage personal information collection and processing, and cope with the risks involved in different scenarios case by case. For privacy protection in the headquarters functional areas, assessments are conducted on legal bases, consent obtaining methods, necessity of information to be collected, minimization of purposes and authorization scope, third-party suppliers' security, reasonableness of retention periods, and IT system security. Based on the assessment results, specific management and control suggestions are provided for scenarios involving risks.

Taking the international third-party customer satisfaction survey as an example, the aim of the survey is to enhance ZTE's services and products based on customer feedback gathered through questionnaire, and thus improve 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

information is accessed, stored, and transferred within the minimum scope; to ensure transparency, the customers are informed of the personal data that is transferred, the processing principles, and their DSRs; and to ensure confidentiality, the personally identifiable data is strictly kept confidential during the survey, and 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 data 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 the corporate governance regulations, 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 mutual-trust relationship with employees, and shaping the image of "employee privacy defender".

The 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 business (including the recruitment website, HR Online, Time & Labor Management System, and HSW), clearly specifying the types of information to be collected, legal bases, DSRs, and ways to exercise DSRs. In addition, the systems mentioned above have met ZTE's baseline requirements for product and information security in the phase of requirement, development, testing, version release, and launch. For offline activities that may involve the collection of the personal information of employees or their family members, privacy notices will be issued in written form to ensure that the employees and their family members fully understand the purpose of data collection and use.

"We Love ZTE" is a teambuilding activity for the family members of overseas employees. Through such activity, ZTE aims to help the employees' family members know about ZTE and improve their sense of recognition and support of the employees' job. In addition, to provide the family members with better services, ZTE collects information on their identity and food habits based on the principle of data minimization, and specifies the information types and purposes of the information collection in the privacy notice. The information is retained in the company's encrypted document library, and only the relevant personnel of the activity have the right to access the library. For example, the team in charge of the transportation has the right to access only the name, telephone number, and flight number of the family members, and cannot obtain other information such as the ID card numbers and food habit information. ZTE also builds partnerships with business travel suppliers to guarantee convenient and efficient services for the family members. Data protection clauses are incorporated into the service agreements with the suppliers to avoid breaches or abuse of personal information. After the activity, the electronic personal data is deleted in a timely manner, and the related paper documents are destroyed directly in strict accordance with the laws, regulations, and

policies of the local countries.

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 employees and external partners of the company, and the personal data involved in the activities is highly sensitive. Therefore, in information-disclosure scenarios such as expense reimbursement, income tax declaration, and securities affairs, personal data shall be protected in an all-round manner to safeguard the personal rights, interests, and privacy of the employees and external partners.

Sticking to the privacy compliance bottom lines of finance and accounting activities not only protects the personal privacy of employees and external partners, but also maintains the company's compliance image. The finance and accounting business units are always 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 make continuous efforts to incorporate the concept of privacy protection into the entire process of financial services, and guarantee compliant personal data processing through organization building and improvement, formulation of regulations and processes, and technical measures. To meet the privacy compliance management requirements, a mechanism is formulated for the review and release of the privacy policy of the Finance Online (FOL) system. In the FOL system, the transmission and storage of personal data are strictly controlled via permission management, and security hardening is conducted. For scenarios such as income tax declaration and securities affairs, all-round regulations and processes are formulated to ensure that each phase of the business meet the compliance requirements for data protection, and the personal rights, interests, and privacy of employees and external partners are protected.

To meet employees' demands for business travel expenses and reduce employees' advanced payment of travel expenses, the company provides channels for employees to apply for business credit cards on a voluntary basis. The expenses incurred due to the commercial activities can be paid by the business credit card, and the consumption records shall be provided for reimbursement. To facilitate employees' expense reimbursement and trace their commercial expenses, the company has interconnected the FOL system with the systems of banks. When the card is used for payment, the consumption records will be synchronized to the FOL system, and the consumption details will be sent to the employee's work email. The related privacy clauses are incorporated into the credit card application form (including the credit card agreement) to keep employees fully informed and obtain the consent of employees. In addition to business expenses, some employees also use the credit cards for personal consumption and make repayments on their own. As the processing of employees' private consumption information lacks a solid legal basis, the company has already taken management and control measures once it knew about the problem. Now the records of employees' private consumption using a business credit card are blocked from the FOL system, protecting employees' privacy while complying with the company's requirements for the business credit card reimbursement.

4.2.9 Strategy and Investment

The strategy and investment business 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. Activities that involve the processing of personal data mainly include the exhibition scenarios, such as holding or participating in exhibitions and forums, inviting customer representatives, and arranging the trips, accommodation, and reception for exhibition participants. An exhibition may involve the processing of a large quantity of personal data, so the data protection compliance management in exhibition scenarios is an important part of ZTE's privacy protection work.

To ensure the lawfulness and compliance of personal information processing in exhibition scenarios, the *Guide to Data Protection Compliance of Exhibition* is formulated, which specifies the management and control measures before, during, and after an exhibition. ZTE has set up key control points for privacy protection in each procedure. Attention is paid to customer invitation and online activity preparations before the exhibition, to venue decoration and guest speeches during the exhibition, and to customer follow-up and customer data deletion after the exhibition. In addition, the relevant business personnel, BU compliance managers, and the data protection compliance experts provide real-time support for privacy protection and data compliance during the exhibition, thereby protecting the personal information of the exhibition participants in an all-round manner.

For example, during the MWC Barcelona, a major international exhibition in the ICT field, ZTE implements compliance management and control on data protection before, during, and after the exhibition, effectively protecting customers' personal data.

(1) Before the exhibition: The *Privacy Notice* is sent to customers along with the *Invitation Letter*. The notice specifies the type and purpose of the personal data to be collected, the protection measures, the rights of the customers, and the ways to exercise the rights. In the scenarios of booking air tickets/hotels/vehicles for customers, the data protection clauses are incorporated into the contracts signed with suppliers, specifying the suppliers' privacy protection responsibilities. On the special website set for the MWC, the privacy policy is displayed, specifying the scope, purpose, storage location, and storage period of the personal data to be collected, which reflects ZTE's compliance with the transparency principle.

(2) During the exhibition: Below the security cameras at the exhibition venue, at the entrances of the venue, in the designated photo-taking area, and next to other equipment with the function of capturing portraits, voices, and other personal data, ZTE posts up reminders to keep customers informed.

(3) After the exhibition: If customer follow-up is conducted via questionnaire after the exhibition, ZTE strictly controls the scope of information collected from customers, and set the name, contact information, email address, and other unnecessary personal information of the customers as optional items. After the exhibition, ZTE deletes customers' personal data collected for the exhibition in a timely manner.

4.3 Openness and Achievement Sharing

ZTE is committed to sharing achievements and promoting exchanges and cooperation. Through forums, seminars, publications, and we-media, ZTE keeps up with 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 build a credible compliance environment together.

ZTE has established its WeChat official account "All About Compliance", and set up the "Data Protection Frontiers" column for privacy protection-related issues. The column focuses on presenting the cutting-edge and trends of data protection compliance, creating a professional platform for research on the laws among countries, addressing the pain points of compliance governance within the industry, and sharing practical practices. The articles published in the column, such as *White Paper on Cross-Border Data Compliance Governance Practice*, *Privacy by Design (PbD) Research Report*, *European Economic Area Regulatory and Enforcement Monitoring*, and *Privacy Protection Compliance Issues During the COVID-19 Pandemic* have been widely recognized in the privacy protection compliance field.

4.4 Key Certifications

ZTE regards privacy protection as the top priority for its products and services, continuously works on strengthening physical, management, technical, and organizational safeguards, and strives to create a sustainable, transparent, open, and trustworthy privacy protection environment.

ZTE attaches importance to authoritative certifications. ZTE headquarters and some subsidiaries have obtained the certification to ISO/IEC 27001:2013 - Information Security Management Systems. The company has also obtained the certification to ISO/IEC 27701: 2019 - Privacy Information Management Systems for human resources management, as well as the terminal, 5G, CN, and digital technology product lines. The 5G product line has passed GSMA's Network Equipment Security Assurance Scheme (NESAS) audit for its development and product lifecycle processes, and some of the 5G products have passed the equipment security assessments of NESAS. In addition, ZTE's 5G RAN solution has obtained the Common Criteria (CC) EAL3+ certification. All these achievements demonstrate that ZTE is dedicated to providing secure, reliable, and compliant telecommunications products and solutions for global customers.

5 Major Events

● Held the second Legal and Compliance Scholars Forum - Seminar on Data Security and Personal Information Protection.	Dec. 2021
● Published the *Privacy by Design (PbD) Research Report.*	Dec. 2021
● Published the *White Paper on Data Cross-Border Compliance Governance Practice.*	Dec. 2021
● Obtained the certification to ISO/IEC 27701:2019 - Privacy Information Management Systems for human resources management.	Sep. 2021
● Obtained the certification to ISO/IEC 2770 :2019 - Privacy Information Management Systems for the terminal products.	Sep. 2021
● Obtained the certification to ISO/IEC 27701:2019 - Privacy Information Management Systems for the iCenter product.	Jul. 2021
● Obtained the certification for ISO/IEC 277. 01:2019 - Privacy Information Management for the core network products.	Jul. 2021

● Published the *ZTE Privacy Protection White Paper (2020)*.	Feb. 2021
● Won the BSI Privacy Strategy Contribution Award.	Dec. 2020
● Published the *Good Practices of Data Protection Compliance of ZTE (2020).*	Dec. 2020
● Incorporated the PbD and privacy by default principle into the R&D process.	Dec. 2020
● Incorporated the PbD and privacy by default principle into the terminal R&D process.	Oct. 2020
● Launched the ZTE Data Protection Compliance Control Landscape.	Jul. 2020
● Obtained the certification to ISO/IEC 27701:2019 - Privacy Information Management Systems for the 5G products.	May. 2020
● Held the "5.25 Data Compliance Annual Meeting 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).*	Dec. 2019
● Won the CACC Excellent Legal Compliance Team of Management Innovation Award.	Nov. 2019
● Launched the Data Subject Rights Response System (DSRRS).	Nov. 2019
● Published the *GDPR Law Enforcement Case Selection White Paper (2019).*	Oct. 2019
● Established the Data Breach and Emergency Response Drill Mechanism.	Jul. 2019
● Held the "Shenzhen Session, China Data Compliance Salon".	Apr. 2019
● Launched the Data Breach Incident Management System (DBIMS).	Apr. 2019
● Incorporated the Compliance Management Platform - Operator GDPR Agreement module into the ZXRDC.	Apr. 2019

Acknowledgement

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

Our heartfelt thanks go to Gao Ruixin, Yang Yuxin, Song Weiqiang, Xu Min, Huang Hao, Wang Zhiyu, Wang Chen, Zhou Yuxin, Mei Aoting, Ding Pei, Wei Andi, Fang Yuan, Huang Hui'e, Jiang Lu, Yang Guirong, Li Huahong, Chi Yifei, Zhao Zhihai, Hui Zhaoshuai, Chen Lisheng, Li Lin, Long Hao, Ma Hua, Xue Yusong, Wang Huan, 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