Implementation Guidelines on EU GDPR and Chinese Cybersecurity Law
Foreword

Basing on the needs of China’s legal service market and Wolters Kluwer’s 180 years of professional service experience, we present 2020 Wolters Kluwer China Law & Reference Compliance Guide Series to China’s legal professionals. Authors of the series are experienced and outstanding teams of lawyer from various practice fields. The 2020 Wolters Kluwer China Law & Reference Compliance Guide Series include four spotlight topics of Cyber Security, Finance, Anti-Bribery and Labor Law. With ideas drawn from multi-dimensional views, we aim to provide practical legal guidance to empower China’s legal community.
Zhong Lun Law Firm, founded in 1993, was one of the first private law partnerships to receive approval from the Ministry of Justice. After years of rapid development and steady growth, today Zhong Lun is one of the largest full-service law firms in China. With over 450 partners and over 3000 professionals working in sixteen offices in Beijing, Shanghai, Shenzhen, Guangzhou, Wuhan, Chengdu, Chongqing, Qingdao, Hangzhou, Nanjing, Tokyo, Hong Kong, London, New York, Los Angeles and San Francisco, Zhong Lun is capable of providing clients with high-quality legal services in more than 70 countries across a wide range of industries and sectors through our specialized expertise and close teamwork. In the field of technology, telecommunication and Internet law, Zhong Lun is highly recommended and ranked the 1st Class by Chambers and Partners, which is a reputable ranking institution worldwide. For several times, Zhong Lun has received key recommendations and awards from the major legal medias such as Legal 500, China Business Law Journal and Asialaw Profiles.

Zhong Lun Cybersecurity and Data Compliance Team is the earliest professional team in China. The partners of Zhong Lun has been invited to the legislative research and discussions of the Internet, cyber security and data protection for many times. The team has developed in-depth cooperation with experts in the field of data compliance all over the world and is good at assisting enterprises establish and optimize the cyber security and data compliance system that meet the requirements of China, EU and other jurisdictions, as well as the information security certification, e.g. CREST, NCSC CHECK, ISO27001, etc.
Mr. Jihong CHEN as an equity partner of Zhong Lun Law Firm, has been practicing and providing legal services for a large number of international enterprises since 1996. He has participated in the research and legislation activities in China related to telecommunications and IT on many occasions, including the Cybersecurity Law, the Regulations for the Protection of Critical Information Infrastructure Security (Exposure Draft), personal information protection rules and related national rules of the People’s Republic of China. Mr. CHEN has published many cybersecurity and data protection related academic works including TMT Law Review, The Legal 500 along with a batch of publications. Mr. CHEN is now the deputy chairman of Cyber and High-tech Committee of All China Lawyers Association (ACLA).

Mr. CHEN specializes in cybersecurity, data protection, telecoms, Internet, IP and other TMT matters. For years, Mr. CHEN was continuously highly recommended as one of the Best Chinese Lawyers by Chambers, Legal500, Legal Band, Asia law and other lawyer ranking agencies in Cybersecurity and TMT area.

Email: chenjihong@zhonglun.com
Ms. Lu HAN as a senior associate of Zhong Lun Law Firm, specializes in the areas of personal information and data protection, cybersecurity, software and hardware, E-commerce and other TMT matters. Her client portfolio covers a wide spectrum of industries including telecommunications and information technology, automobile, insurance, medical and life science, new energy resources, real estate, retail and manufacturing.

Email: hanlu@zhonglun.com
Ms. Run YANG specializes in GDPR, data protection, cybersecurity, TMT and IP matters. She has participated in multiple projects regarding cybersecurity and data protection compliance for well-known enterprises with practical experiences.

Email: evayang@zhonglun.com
Special Thanks to Experts and Co-authors of Part I.

Dr. Dennis-Kenji Kipker

Scientific Manager of the IGMR at the University of Bremen, Executive Director of Certavo GmbH - international compliance management, Legal Advisor of CERT@VDE, Frankfurt am Main, Member of the Board of the European Academy for Freedom of Information and Data Protection (EAID) in Berlin.

Email: kipker@uni-bremen.de
Researcher of the IGMR, lecturer in civil law. His main areas of research are the legal regulations of data protection, cybersecurity, communication, telemedia and general civil law, especially contractual and legal obligations.

Email: mwalkusz@uni-bremen.de
# Table of Content

Preface ......................................................................................................................................... 1

**PART I Challenges of GDPR and the Difference of Data Protection in China and EU** ......................................................... 3
  1. How GDPR Protect Personal Data .................................................................................. 3
  2. Whether Your Company Fall under the Jurisdiction of GDPR ................................. 6
  3. How to Collect and Process Personal Data in a Compliant Manner .................... 7
  4. Rights of Data Subjects under GDPR ...................................................................... 11
  5. Obligations of Data Controller and Processor .................................................... 15
  6. Cross Border Data Transfer ...................................................................................... 22
  7. GDPR Compliance Strategy for Companies ...................................................... 23
  8. Risks Reflected in GDPR Enforcement Cases ................................................... 27

**PART II How Chinese Companies Comply with GDPR Compliance ................. 35**
  1. Tendency: Progress in the Interpretation of GDPR .............................................. 35
  2. Under Which Circumstances Will GDPR be Applied out of EU?
     — An Interpretation on EDPB Guidelines on the territorial scope of the GDPR (Article 3) ................................................................. 44
  3. What is Valid Consent under GDPR
     — An Interpretation on EDPB’s Guidelines 05/2020 on consent under Regulation 2016/679 ................................................................. 49
  4. What is “Necessary for the Performance of a Contract” under GDPR
     — An Interpretation on EDPB Guidelines 2-2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects ........................................ 54
5. What is Data Protection by Design and by Default  
   —An Interpretation on EDPB Guidelines on Article 25 Data Protection  
   by Design and by Default .......................................................... 57

6. The Application of GDPR in the Scenario of Video Devices  
   —An Interpretation of EDPB Guidelines on processing personal data  
   through video devices......................................................................... 69

7. Personal Data Risks and Countermeasures in the Context of IoV under GDPR  
   —An Interpretation on EDPB Guidelines on processing personal data  
   in the context of connected vehicles and mobility related applications .. 74

8. Eight Data Protection Key Words of Smart Home Launching out .......... 81

PART III Cyber Security and Data Compliance Localization Requirements  
for EU Companies Entering Chinese Market ................................. 90

1. Rules on Personal Information Protection........................................ 90

2. Multi-level Protection Scheme ...................................................... 94

3. The Critical Information Infrastructure Protection System............... 99

4. Rules on the Protection of Important Data ..................................... 104

5. Internet Real Name System and Regulation on User Information Release 106


7. The Cryptographic Product Management System ........................... 111
Since GDPR came into effect in 2018, it has gradually become an important reference for data protection legislation in various countries and has had a profound impact on the development of overseas markets for Chinese companies. At the same time, China has constantly established a core legal system of cybersecurity and data compliance with wide coverage and high levels of effectiveness. Both domestic and oversea companies in China are required to fulfill a series of cybersecurity and data protection obligations.

In this context, in order to help companies more systematically and efficiently solve the data compliance challenges they will face when going abroad or coming to China, Wolters Kluwer and Zhong Lun Law Firm jointly issue the Implementation Guidelines on EU GDPR and Chinese Cybersecurity Law providing systematic practical guidance for companies.

The Guidelines mainly include three parts:

Part I Challenges of GDPR and the Difference of Data Protection in China and EU is the foundation for the implementation of GDPR compliance of companies launching out. This Part comprehensively introduces the compliance requirements of GDPR and the compliance challenges that Chinese companies may face when developing overseas markets and sorts out the typical cases of GDPR enforcement in the past two years with the summary of the common punishment reasons for companies' reference.

Part II How Chinese Companies Comply with GDPR Compliance is the main focus for the implementation of GDPR compliance of companies launching out. The content of this Part explains the relevant guidelines of GDPR in detail through seven specific topics, including general issues such as applicability determination and legal basis selection, as well as special requirements in the certain fields such as connected vehicles and smart homes, etc., and systematically interprets the key points of company's compliance.

Part III Cyber Security and Data Compliance Localization Requirements for EU Companies Entering Chinese Market is a comprehensive overview of localization for companies coming
to China. This Part describes the overall system of China's cybersecurity and data compliance and outlines seven critical systems including the multi-level protection scheme, rules on personal information and important data protection, etc., providing basic guidance for EU companies to achieve localized cybersecurity and data compliance in Chinese market.

For companies, the trend of strict data compliance supervision around the world is both a huge challenge and a valuable opportunity. The Guidelines hope to provide detailed guidance on compliance implementation for companies through comprehensive introduction, systemic interpretations, and practical advice on GDPR and China's cybersecurity and data compliance legal system.
PART I

Challenges of GDPR and the Difference of Data Protection in China and EU

1. How GDPR Protect Personal Data

1.1 Overview of the Legal Framework of GDPR

Since 25th of May 2018, the General Data Protection Regulation (GDPR) forms the new legislative framework of data protection in the EU. By coming into effect, GDPR repeals the EU Directive 95/46/EC of the European Parliament and of the Council of 24th of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. EU Directives, in contrast to EU Regulations, are not directly binding for the Member States. Furthermore, it is the obligation of the Member States to transfer the principles of the Directive into their respective national law. As a result, the Member States implemented the Directive in different ways, so the data protection level in the EU became partially unequal and inconsistent, which led to legal uncertainty and intransparence for companies operating in the EU. GDPR shall solve this problem by ensuring a ‘consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union. It is also prescribed that ‘the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States’. In comparison to the Cyber Security Law of the People’s Republic of China (CSL), which protects among other aspects the cyberspace and national security, GDPR only focuses on the rights on personality and (intellectual) property of natural persons.
There is another difference: Whereas the Chinese legal data protection framework mostly consists of one central law, concretised by several sublegal norms as well as technical standards, the EU data protection framework depends on a variety of legal norms, mostly based on several branch and topic specific regulations, which can partially be defined by the EU Member States as well. This is legally possible due to so called ‘opening clauses’ in GDPR, which allow the Member States to regulate some aspects of the data protection framework on their own. This partial national legislation, which is often addressed by special laws, causes the EU data protection framework to be much more difficult and less clear than politically intended by the creation of the EU GDPR. For example, data controllers are allowed to process data when it is necessary to fulfil a legal obligation. For these legal obligations, the Member States are allowed to create more specific provisions determining precisely the requirements for the processing to ensure a lawful and fair processing of data, especially in the sectors of health and social law. For example, in Germany, doctors and hospitals that cooperate with the statutory health insurance, have the obligation to process patient data if it is necessary for quality assurance. As a result of the co-regulation in EU data protection law, the controller must observe all national regulations which are applicable in his certain case in addition to EU law to be fully compliant.

With regard to the EU data protection framework and besides GDPR, the ePrivacy Directive is mentionable as well. This Directive provides concrete and strict protection rules for the processing of personal data which is being transferred by electronic and regulated communication services. According to article of 95 GDPR, the regulation does not establish additional obligations for controllers of data, if they already follow the special regulations of the ePrivacy Directive and if the concrete section of the Directive protects the same interests as the GDPR. The partially outdated ePrivacy Directive of 2002 will be replaced by the ePrivacy Regulation. The ePrivacy Regulation was meant to become law in parallel with GDPR, but serval severe political disputes led to the decision of the EU legislator to postpone the validation of the new law. The draft of the ePrivacy Regulation expands the personal scope of application compared to the Directive, as it also affects, next to electronic communication services, so called ‘over-the-top-communication services’. These are defined as providers of communication services in the Internet without operating the communication infrastructure, such as e-mail- or messenger-providers. If the draft version of the ePrivacy Regulation will be adopted, it replaces the Directive and all references to the Directive shall affect the Regulation. Regarding the interaction with GDPR, the draft of the ePrivacy Regulation declares that it clarifies and completes the general terms of GDPR. But, in detail, many aspects of the scope of applicability of GDPR and ePrivacy Regulation still remain unclear, as well as the schedule for the adoption of the ePrivacy Regulation.

1.2 Keywords of Personal Data Protection

(1) Personal Data
According to Article 4 of GDPR, personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Under the data protection framework in China, personal information is defined as means any information saved in an electronic form or otherwise, that can independently or together with other information to identify a natural person or reflect the activities of a natural person, including but not limited to name, dates of birth, identification numbers, personal biometric information, addresses, contact information etc.. In addition, the GB/T 35273-2020 Information Security Technology National Standard: Information Security Technology - Personal Information Security Specification also clarifies the method of identifying personal information and specifies the categories of personal information. According to the relevant provisions, any information that can identify specific person directly or indirectly combined with other information may fall into the scope of personal information.

(2) Special Category of Personal Data

According to Article 9 of GDPR, special category of data refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. In principle, processing this kind of data is prohibited.

The parallel concept under data protection framework in China is personal sensitive information, the scope of which is wider compared with that of special category of personal data. Personal sensitive information refers to any personal information that, once divulged, illegally provided or misused, may endanger personal and property safety and is very likely to cause harm to or discrimination against personal reputation and physical and mental health, etc.

(3) Data Controller and Processor

According to Article 4 of GDPR, data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data while data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The concepts of “controller” and “processor” under data protection framework in China are
basically the same to those under GDPR. “controller” means an organization or individual who is capable to decide the purpose and methods of processing personal information while “processor” means the organization or individual who conducts the personal information processing activities under controller’s instruction.

2. Whether Your Company Fall under the Jurisdiction of GDPR

To determine whether a company will fall within the scope of GDPR is a basis for GDPR compliance. The company shall take the requirements of both objective scope as well as geographic scope into consideration when determining.

2.1 Objective Scope

According to Article 2 of GDPR, GDPR applies to the processing of personal data wholly or partly by automated means and to the processing of personal data by other than automated means which form part of a filing system or are intended to form part of a filing system, that is, GDPR applies to the processing of personal data. Your company will not fall within the scope of GDPR if no personal data is involved in the data processing activities.

2.2 Geographic Scope

There are two standards for the determination of geographic scope: establishment criterion and targeting criterion.

According to Article 3.1 of GDPR, establishment criterion means GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in EU, regardless of whether the processing takes place in EU or not.

According to Article 3.2 of GDPR, targeting criterion means GDPR applies to the processing of personal data of data subjects who are in EU by a controller or processor not established in EU, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in EU; or (b) the monitoring of their behavior as far as their behavior takes place within EU.

Compared with the application determination of GDPR, under the data protection legal framework in China, any entities involved in the establishment, operation, maintenance and use of the Internet as well as the supervision and management of cyber security within the territory of the People’s Republic of China shall comply with all requirements of CSL.
3. How to Collect and Process Personal Data in a Compliant Manner

3.1 Principles of Processing Personal Data

Similar to the data protection legal framework in China, GDPR establishes the basic principles for processing personal data. Every processing must be executed according to the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability. It is important to mention that these principles are not only basic rules or program sets for optimization. Indeed, they are mandatory obligations for the controller, so that non-compliance to these specifications may be sanctioned. These basic principles of the processing of personal data are codified in Article 5 of GDPR:

(1) Legality, processing in good faith and transparency

Every processing of personal data must be covered by a legal basis or consent of the data subject. Also, it must be possible for data subjects to understand what happens to their personal data. This includes that the data subject is able to get information about the identity of the controller, the purposes of the data processing, the category of information being processed, and the risks, applicable laws and regulations, as well as the affected rights with regard to the processing of personal data. Every information must be easily accessible and easily understandable for the person concerned.

(2) Earmarking

Personal data must be collected for defined, clear and legitimate purposes and may not be further processed in a manner incompatible with these purposes. If the controller is carrying out further processing activities, it has to be ensured that the operations are compatible with the original processing purpose. If a controller wants to change the purpose of the processing of data (for example online shops, which originally received personal data in order to complete a transaction/fulfil a contract, and are now planning to use the same personal data for reasons of personalised advertising), the controller has to be compliant with the conditions of Article 6.4 of GDPR.

(3) Data minimization

Data collection should be limited to what is necessary for the purpose of processing. So, the processing of personal data has to be reduced to the lowest level possible in relation to the purpose of processing.

(4) Accuracy
Processed data must be factually correct and up-to-date. Every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without undue delay.

(5) Storage limitation

Personal data is to be kept in a form which permits the identification of data subjects for no longer than it is necessary for the purposes for which the personal data is processed. Companies should establish data retention policies that define which data is stored and how this is to be done in accordance with data protection regulations.

(6) Integrity and confidentiality

Data controllers must ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (TOM).

(7) Accountability

The controller is responsible for compliance with the above mentioned principles. In addition, the controller has to ensure and to prove with all accessible measures, that the processing of personal data is harmonised with the GDPR.

3.2 Legitimation for the Processing of Personal Data

As mentioned before, personal data must be processed in a lawful manner. Under GDPR, the processing of data is only permitted, if the data subject declares his/her consent or if there is a legal basis for processing the data related to the person. This means that unlike the data protection legal framework in China, personal data processing is not only based on consent. According to Article 6 of GDPR, there are 6 legal basis for the processing of personal data, which can be divided into the following two categories:

(1) The Consent of Personal Data Subject

The consent is an important legal basis with detailed requirements under GDPR. It is defined as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her”. When the personal data processing is based on the consent of subjects, the controller bears the burden of proof for a given consent, especially for online consents. The consent can generally be made in any form - verbally, in writing or electronically as long as the consent of the data subject is clearly expressed. So, declaring a consent is even possible with a clear action of the affected person.
In addition, the consent must be given voluntary. This is not the case if the person concerned has no real or free choice or is not in a position to refuse or withdraw his consent without suffering disadvantages as a result. When assessing whether the consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, is conditional on the consent to the processing of personal data that is not necessary for the performance of that contract. So, granting of consent may not be used as a condition for contractual services (‘prohibition of tying-in’). Furthermore, according to the definition mentioned in Article 7 of GDPR, the consent requires an informed statement of intent by the data subject in the individual case. The person concerned should therefore be aware of at least the basic information of the data controller and the purposes for which the personal data will be used. The data controller shall inform the data subject his right to declare withdrawal at any time prior to the consent is given. The controller must also ensure that the withdrawal is as easy to declare as the consent.

Another critical aspect with regard to the consent is the consent of a child. Children are, due to their lack of cognitive faculty, in general not able to give lawful agreements. According to Article 8 of GDPR, the minimum age for effective consent of a child is 16 years. If the child is below that age, data processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. Meanwhile, member states may provide special regulations regarding the consent of a child.

(2) Other legal basis

The processing of personal data can be carried out on other legal basis mentioned in Article 6 of GDPR, if there is no consent of the data subject:

- Performance of contract: The processing is necessary for the performance of a contract to which the person concerned is a party. ‘Performance of a contract’ means any processing of data in a contractual context (irrespective of the stage of the contract). Data processing in accordance with Article 6.1.(b) of GDPR may also be necessary to carry out pre-contractual measures on request of the person concerned. The need is determined by taking into account the purpose of the processing and the contractual clauses. The requirement of the necessity must be interpreted very closely. The processing of personal data is only necessary for fulfilling a purpose if a contract cannot be performed without it. For example: A company, which runs an online shop has to process at least the name, address and payment information of a customer to fulfil a purchase contract.

- Legal obligation: The processing is necessary to fulfil a legal obligation to which the controller is subject. This means especially not an obligation which is established by a
private and autonomous decision. A legal obligation can be founded in a law of a Member State, as well as by the European Union law.

- Vital interests: The processing is necessary to protect the vital interests of the data subject/another natural person. This clause was established for emergencies, but it is not only applicable in cases of risks of death. Named examples for the usage of this clause are medical emergencies, surveillance of epidemics or organisational measures in cases of natural disasters.

- Public interests: The processing is necessary for the performance of a task in the public interest or in the exercise of official authority conferred on the controller. This clause is purposed to allow public authorities to process data and has no significant meaning for data processing by private persons or institutions.

- Legitimate interests: The processing is necessary to safeguard the legitimate interests of the data controller or a third party, unless the fundamental rights and freedoms of the data subject requiring the protection of personal data prevail. In this context it is important to mention, that the controller bears the burden of proof for the legitimate interests. The legitimate interests are measured on one hand by the purpose for which the data is processed, and on the other hand by the intervention intensity which is caused for the affected person. Economic interests are indeed lawful interests, but it must be noted that rights on the personality of humans are privileged. The more intervention-intensive the data processing measures are, the likelier it is that the person concerned has an interest in the exclusion of data processing outweighing the controller’s interests. Special categories of personal data are deprived of a general outweighing of interests due to their particular sensitivity for the right on personality from the affected people.

3.3 Special Category of Personal Data

Compared to the general category of data, the processing of special category of personal data shall comply with stricter requirements. According to Article. 9 of GDPR, special category of personal data refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. In principle, processing this kind of data is prohibited and the permissions mentioned in Article 9.2 of GDPR are to see as exceptions. Examples for such an exception of the prohibition principle are the following:

- Consent: The consent must be given to specific personal information by the personal data subject concerned and the consent must be explicit and conform the requirements of GDPR.
• Labour law and social law: The processing is necessary to enable the data subject to exercise his or her rights under labour law, social security law and social protection law.

• Protection of vital interests: The processing is necessary to protect the vital interests of the data subject or another natural person and in the case when the data subject is unable to give his consent for data processing due to physical or legal reasons.

• Data obviously made public: The processing relates to personal data which the data subject has obviously made public based on a free decision.

• Enforcement of legal claims: The processing is necessary to assert, exercise or defend legal claims or in the case of acts of the courts within the framework of their judicial activity; in this context, a careful balancing of interests is required.

• Research purposes: The processing is required on the basis of EU or EU Member State law for scientific or historical research purposes or for statistical purposes.

4. Rights of Data Subjects under GDPR

The rights enjoyed by data subjects under GDPR are similar to those under CSL in China. According to GDPR, the rights enjoyed by data subjects are provision of information, right to access, right to rectification, right to erasure (also referred to as right to be forgotten), right for data portability, right to restriction of processing, right to object and right to object automated processing.

4.1 Provision of Information

The controller must provide to the data subject relevant information for processing before carrying out the processing activity. Concerning the provision of information, the GDPR distinguishes between two different options: when personal data is gathered directly from the data subject, Article 13 of GDPR shall apply. In this case, the person has to participate in the collection process in a visible way (physical, mental, active or passive). In the case where personal data has not been obtained from the data subject, Article 14 of GDPR shall apply.

The controller must inform the data subject of name/contact details of the controller (if applicable), the name of the representative (if applicable), contact details of the data protection officer (DPO) (if applicable), uses and legal bases for the processing of personal data, recipients of personal data (if there are recipients), information on cross border data transfer, duration of storage of personal data, rights of data subjects, rights to withdraw consent, legal or contractual obligations to provide personal data, information on the existence of automated decision-making including profiling and so on.
4.2 Right of Access

Sense and purpose of the right of access to the processed data is to increase the fairness and transparency of the data processing and create the possibility for data subjects to verify the legality of the processing operations carried out with their personal data. The right of access can be claimed by every person. Even in the case when a controller does not have any information about the claimant, it is his duty to inform the data subject about that fact. If the controller is in possession of personal data of the claimant, the controller provides the person concerned with a copy of all data which is being stored.

The right of access has to include at least the following information: processing purposes, categories of personal data to be processed, the recipients to whom the data have been/are still being disclosed (especially in the case of third countries), the planned storage period or the criteria for determining the duration, the existence of a right of appeal to the supervisory authority, intended consequences of automated decision-making, information on cross border data transfer of personal data.

4.3 Right to Rectification

Referring to the fact that wrong information can result in a false (digital) image of a person, which could be harmful for the development of the personality and the public perception, the accuracy of processed personal data is an important aspect. To avoid such scenarios, GDPR constitutes a claim against the controller to correct any wrongly processed data, irrespective of whether the data has been wrong from the beginning of the processing or if it became wrong later on. The data subject has also the right to complete the data saved by the controller. The assessment whether a database has been completed depends on the individual case. If missing data is necessary to fulfil the purpose for which the data originally has been collected for, then it must be added to the database upon request.

4.4 Right to Erasure/ Right to be Forgotten

(1) Right to Erasure

The controller has the obligation to erase the data concerning a person immediately, if the affected person demands for it. The personal data must be erased in a way which makes it impossible to restore the deleted information. As a result, the physical destruction of the medium containing the data would be sufficient, but not moving it into the trash bin of the operating system or a simple hint that the perusal of the information is no longer allowed. In the following situations, the affected person has the right to erasure:

- The personal data is no longer necessary in relation to the purposes for which the data has been collected or otherwise processed;
• The data subject withdraws the consent on which the processing is based and when no other legal justification for the processing of personal data can be given;

• The data subject objects to the processing successfully and there is no overwhelming justifiable reasons to continue the processing;

• The personal data has been processed unlawfully;

• The personal data has to be erased for compliance with a legal obligation of the EU or a Member State law to which the controller is subject.

The right to erasure does exceptionally not apply if the data processing is necessary in case of the following circumstances:

• Exercising the right of freedom of expression and information;

• Compliance with a legal obligation which requires the processing of personal data by the EU or a Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

• Reasons of public interest in the area of public health;

• Achieving purposes in the public interest, scientific or historical research purposes or statistical purposes;

• Establishment, exercise or defence of legal claims.

The controller must communicate any rectification or erasure of personal data to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients, if the data subject requests for it.

**(2) Right to be Forgotten**

The obligation to erasure does not include copies of data which are in the possession of third parties. For this reason, the controller must, taking account of available technology and the cost of implementation, take reasonable steps, including technical measures, to inform controllers that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. The right to be forgotten especially includes publications on the internet. The publisher has the duty to inform possessors of the affected data that are outside of the scope of application of GDPR as well. As a result, the
publisher is obliged to do his best efforts to erase every track of the information spread on the internet.

A typical example for the use of the right to be forgotten would be the following case: A data controller publishes personal data about an individual on its website. The data can be found by entering the name of the person concerned into an online search engine - which means that an unlimited number of people can access it, so that the data has been published by legal definition. If the person concerned exercises the right to be forgotten, the company must take appropriate measures to inform the search engine operator about the request. The burden of proof that no other reasonable steps are possible is on the publisher.

4.5 Right to Restriction of Processing

Data Controller shall continue processing personal data only under limited circumstances if personal data subjects restrict the processing of his/her personal data. Personal data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, there is a period enabling the controller to verify the accuracy of the personal data;

- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

- the data subject has objected to processing and there should be the verification whether the legitimate grounds of the controller override those of the data subject.

Under the above-mentioned circumstances, data controller shall stop the processing of personal data unless the consent of personal data subject has been obtained or such processing is for purposes in the public interest, establishment, exercise or defence of legal claims defending rights of individual or legal entities.

4.6 Right to Data Portability

With the right to data portability, GDPR enables an easy switching of service providers with the possibility to move, copy or transfer personal data from one IT environment to another. GDPR prescribes the right of the data subject to receive the personal data that has been provided to a controller in a structured, commonly used and machine-readable format, so
that it can be transmitted to another controller without any hindrance of the previous one, when the data processing is based on a consent or a contract and if the processing is carried out by automated means. If it is technically possible, the data subject has also the right to have the personal data directly transmitted from one controller to another. An example of how the right to data portability could be used would be the following case: The operator of a social network receives the request of a user to transmit his profile to the operator of another social network (name, e-mail address, age, place of residence, photos, comments, thoughts, chats). According to the right to data portability, the company should transmit the personal data of the user; however, some data may also concern third parties (e.g. chat protocols) - this kind of data may not be transmitted to the operator of another network due to the third party interests involved.

4.7 Right to Object

The right to object is not a right for terminating an unlawful processing of personal data, its purpose is to end a legally compliant processing of the data concerned. The data subject has the right to object, on grounds relating to the individual particular situation, at any time of processing personal data which is based on public or legitimate interests. In case of objection, the controller must not process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. GDPR also prescribes a right to object if the personal data has been processed for purposes of direct marketing. The controller has the obligation to inform the data subject about the right to object at the latest time of the first communication and shall bring it explicitly to attention.

4.8 Right to Object Automated Processing

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects concerning him/her. Similarly, there are exceptions to such right. The provision shall not apply if the decision is necessary for entering into, or performance of, a contract between the data subject and a data controller; is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or is based on the data subject’s explicit consent.

5. Obligations of Data Controller and Processor

5.1 General Requirements
(1) Data Protection Officer

If the core processing operations require regular and systematic monitoring of the data subjects in a large scale or if the core processing operations consist of processing on a large scale of special categories of personal data or personal data relating to criminal convictions and offences, the controller and the processor must designate a data protection officer (DPO), who is responsible for involving the data protection officer in all issues which relate to the protection of personal data in a properly and timely manner. The controller and the processor are responsible for involving the data protection officer in all issues which relate to the protection of personal data in a properly and timely manner. The controller and processor support the data protection officer in performing his tasks by providing the resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his expert knowledge. Also, it must be ensured that the data protection officer does not receive any instructions from the controller or processor regarding the exercise of his tasks. The data protection officer must not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor. The data protection officer must fulfil at least the following tasks:

- inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to GDPR and to other EU or Member State data protection provisions;

- monitor compliance with GDPR, with other EU or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

- provide advice where requested with regard to the data protection impact assessment;

- cooperate with the supervisory authority;

- act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation, and to consult, where appropriate, with regard to any other matter.

(2) Representatives

For data controllers or processors not established in the Union but regulated by GDPR due to the offering of goods or services to data subjects in the Union or the monitoring of data subjects behaviour which takes place within the Union, the data controllers or processors shall delegate representatives in the Union. Unlike neutral data protection officers, the
European Representative is primarily responsible for the following:

- represent data controllers and processors to perform GDPR compliance obligations in the Union;
- perform their duties in accordance with the delegations of the data controller and processor; and
- maintain records of processing activities carried out in representation of data controllers and processors.

(3) Record of Processing Activities

Each controller and processor must maintain a written record of processing activities under his responsibility. The records must be created and saved in a way that makes it possible for the supervisory authority to observe the data processing, if necessary. The records have to include at least the following information:

- name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- purposes of the processing;
- description of the categories of data subjects and of the categories of personal data;
- categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and information on the transmission mechanism;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures.

The records must be kept in written or electronic form.

(4) Data Protection Impact Assessment

The controller must carry out a prior assessment of the impact of the proposed processing operations on the protection of personal data (DPIA) where the nature of the processing
likely to pose a high risk to the rights and freedoms of data subjects. For this purpose, the controller seeks the advice of a data protection officer. The assessment covers the content of processing operations from their preparation to their subsequent impact. GDPR mentions four examples of risky data processing activities:

- systematic and comprehensive assessment of personal data;
- processing of special categories of personal data;
- surveillance of publicly accessible areas;
- operations aimed at processing large amounts of data at regional, national or transnational level.

In addition to the typical circumstances mentioned above, an assessment is also required in the case of the use of automatic processing technologies in the processing of personal data, the processing of children’s personal data, and the collection and processing of personal data from different sources or different databases.

The assessment must contain at least:

- data Reflection: systematic description of the envisaged processing operations and the purposes of the processing;
- necessity assessment: assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- risk assessment: assessment of the risks to the rights and freedoms of data subjects;
- description on measurement: measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

(5) Privacy by Design and by Default

According to the requirements of GDPR, at the time of first decision on the purposes and manners of the design and throughout the whole process of data processing, the data protection obligations by design and by default shall be fulfilled so as to ensure continuous compliance.

- Privacy by Design
In view of the fact that an adequate protection of privacy in the digital age is not possible without privacy-compliant technology design, the controller has the obligation to install security and privacy measures already in the process of creating a data processing system. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller must, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures (TOM). These TOM are designed to fulfil data-protection principles as a preventive measure in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of GDPR and to protect the rights of data subjects. This also means that TOM should not be executed only after a data breach.

Technical measures can be defined as all arrangements and procedures that are in relation to the processing of data, such as the removal of data carriers, structural measures intended to prevent the entry of unauthorised persons, or security measures, such as hardware and software checks, access control, encryption or password security. Organisational measures are aimed in particular at the external framework conditions for the design of the technical process, such as observance of the four-eyes principle, logging of activities and sampling routines. Examples for a successful privacy design could include secure user authentication solutions, anonymisation and pseudonymisation techniques, integrated encryption methods, the limitation of data processing to the absolutely necessary level (data saving) and especially for the area of networked automobiles the separation of identification and content data, e.g. concerning the use of location-based services.

- Privacy by Default

The principle of Privacy by Default commits the controller of the personal data to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is used. In consequence, the data subjects shall receive the highest possible level of privacy in general, without the needs to change the privacy settings first. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. If users still want their personal data to be used, they have to change the settings independently. According to Privacy by Default, such a setting must be done with an opt-in selection system, to make sure that the affected person is aware of the disposition of his privacy.

(6) Data Breach Notification

In case of a data breach, the controller has the obligation to notify the supervisory authority and the affected persons. The notification must be performed without undue delay and,
where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The notification must contain at least:

- nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

- name and contact details of the data protection officer or other contact point where more information can be obtained;

- likely consequences of the personal data breach;

- measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

A data processor must inform the controller about a data breach in the same way.

5.2 Substantive Requirements for Data Processing

Based on the fundamental obligations mentioned above, the substantive requirements shall be met when data controllers and data processors carry out data processing activities can be summarized as:

- every processing of personal data must be covered by a legal basis or consent of the data subject and fulfill all mandatory obligations of GDPR;

- in cases where a cross-border data transfer is involved, in addition to compliance with the requirements of legal basis and principles, it is also necessary to adopt appropriate transmission protection mechanisms; and

- the realization of the aforesaid basic requirements shall be guaranteed by the internal technical management measures, procedures and systems of the company as well as by the public-announced privacy policies and privacy settings. Companies shall also prudently sort out and classify the data processing actions according to the business models, data flows and targeted user groups, to ensure there is appropriate legal basis and appropriate modes of presentation to satisfy the requirements of the GDPR.

5.3 Obligations of Joint Controller and Data Processor

(1) Joint Controller
Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. In such case, the joint controllers shall, in a transparent manner, clarify their corresponding responsibilities for complying with the GDPR compliance requirements and, in particular, clarify the guarantee of the exercise of rights of personal data subjects.

In order to guarantee the legitimate rights and interests of personal data subjects, the joint controller shall take appropriate means to inform personal data subjects of the arrangement made by the joint data controllers with respect to the division of responsibilities. In addition, according to GDPR, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers regardless of what agreement is made among common data controllers.

(2) Data Processor

Where the processing activity is to be carried out on behalf of a controller, the controller must use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner, that processing will meet the requirements of GDPR and ensure the protection of the rights of the data subject. The legal possibility of engaging a processor shall simplify data processing for the controller, if it is too complex or extensive for him, but it establishes strict data protection measures with regard to the outsourcing process. So, the economic interests of the controller and the personal interests the affected person are balanced in a lawful way. If a controller wants to outsource his processing activities, he must ensure that the processing by a processor must be governed by a contract or other legal act under EU or Member State law, that is binding on the processor with regard to the controller and that sets out the following aspects:

- duration of data processing activities;
- nature and purpose of the processing;
- Type of personal data and categories of data subjects;
- obligations and rights of the controller;
- the processor shall process the personal data only on documented instructions from the controller, unless it is required to do so by EU or Member State law to which the processor is subject;
- the processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
• all data security requirements are observed;

• the processor shall not engage a data processor for himself for processing the controller’s data without the permission of the controller in written form. If the processor engages another processor, he has to ensure the same contractual measures;

• the processor must, taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller’s obligations established by GDPR, in particular to respond to requests for exercising the data subject’s rights;

• the processor must, at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services relating to processing, and delete existing copies unless EU or Member State law requires storage of the personal data.

• the processor makes available to the controller all information necessary to demonstrate compliance and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

The contract between controller and processor must be in writing, including electronic form.

6. Cross Border Data Transfer

Any transfer of personal data to a country or region outside the EU/ European Economic Area is the cross-border transfer of personal data under GDPR, and thus it is required to adopt appropriate transmission protection mechanisms, regardless of whether the personal data is physically transferred or accessed remotely. In general, there are three kinds of transmission protection mechanisms commonly adopted in practice:

6.1 Adequate Decision

Where the European Commission takes the view that adequate level of protection can be ensured by a particular country, region, sector or international organization, personal data may be stored in that country or region without special authorisation. The Commission of the EU declared Andorra, Argentina, Canada (only commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan and the USA (if the recipient belongs to the Privacy Shield) as secure countries. The data transfer to these countries is expressly permitted.

6.2 Binding Corporate Rules (BCRs)

---

Binding corporate rules apply to the inter-group transmission of personal data and shall be subject to the approval of supervisory authority. These rules are legally binding and shall be implemented by the group members and their employees. Binding company rules shall at least contain the following contents:

- name and contact details of member of the specific member applicable;

- type of personal data involved in the cross-border transfer under this rule, category of personal data subject; category and purpose of the processing, etc.

Standard Contractual Clauses

Conclusion of standard contractual clauses for cross-border personal data transfer is currently a widely adopted transmission protection mechanism by companies. The EU Commission have formulated standard contractual clauses which applies to different data processing roles. Such clauses have specified the rights and obligations of data providers and data recipients with respect to the cross-border personal data transfer. Basic information of both parties, such as the purposes of transfer, categories of personal data subjects involved, categories and numbers of personal data and the security measures adopted shall be supplemented at the time of execution.

At present, the standard contractual clauses are formulated by the EU Commission, and the data protection regulators of member states of EU are likely to issue other versions of the contract clauses, on which a close eye shall be kept.

7. GDPR Compliance Strategy for Companies

7.1 GDPR Compliance Risks

(1) Consequences of non-compliance

Each EU Member State has its own national supervisory authority which is responsible for carrying out the tasks on the territory of its own Member State. When supervisory authority performs its duties, and the following aspects will be taken into account:

- processing operations often involve several Member States, so that several supervisory authorities might be in charge at the same time;

- in order to avoid multiple responsibilities, there is a ‘one-stop shop’, from which the responsibility of a single supervisory authority results;
• a leading supervisory authority serves as the sole contact for the controller/processor on questions concerning the cross-border processing techniques carried out by it

It shall be noted by Chinese companies that for data controllers or data processors which are not established within EU but governed by GDPR in accordance with Article 3 of GDPR, the following factors may be considered in the determination of the governing supervisory authority: in which country are data processing activities mainly conducted? in which country are the subjects concerned mainly located? and which country’s data protection agency has received the complaint from the personal data subjects?

Supervisory authorities have the right to impose penalties based on GDPR and in accordance with specific laws and regulations of the member country concerned. According to GDPR, a fine of up to 10,000,000 euros or an amount equivalent to 2% of the child’s total global turnover of the previous year may be imposed, whichever is higher, in violation of rules on child consent; data protection by design and by default; joint data controller, establishment of representatives, record of data processing, cooperation with supervisory authorities, data security measures, notice of data leakage, data protection impact assessment as well as data protection officer. A fine of up to 20,000,000 euros or an amount equal to 4% of its total global turnover of the previous year may be imposed, whichever is higher, against the violation of relevant provisions on basic principles and legal basis for data processing activities, rights of the data subject, cross-border data transfer, as well as provisions of the laws of the member states and orders of supervisory authority.

(2) Risks for GDPR Application

For Chinese companies, the determination of the applicability of GDPR as well as the applicable business scope is the first step for the implementation of GDPR compliance work. GDPR applies not only to institutions established in Europe, but also to companies with target customers in EU. With respect to the latter, specifically, this includes the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, as well as the monitoring of their behavior as far as their behavior takes place within the Union.

Based on the above-mentioned provisions, a Chinese company which has established a representative office or branch within the territory of the EU is required to determine whether or not the established office or its personnel constitute its place of business as a result of the conduction of substantive business activities. A Chinese company is not established within the territory of the EU is required to determine whether or not to offer goods or services to personal data subjects within the territory of the EU, or whether or not it constitutes monitoring of the behavior of the personal data subjects. The monitoring includes various forms, such as online tracking by use of cookies or other tracking technologies, market research based on user profiles, etc.
(3) Risks for GDPR Compliance

As previously mentioned, any violation of the compliance requirements of GDPR may lead to high penalties. Under GDPR, where a data controller or processor violates relevant provisions or basic principles of data processing and provisions on lawfulness of processing and thereby harm the rights of data subjects, the data subjects have the right to directly raise a complaint with the supervisory authority, and the supervisory authority may decide whether to provide the data controller or processor with channels for judicial remedy or impose administrative penalties on the data subject who violates the provisions.

In addition to the punishment imposed by the supervisory authority, the duration of violation may have a relatively significant impact on commercial interests and goodwill. As for the risk level that the company may face, the company may carry out assessment in combination with the specific situation of the EU market. In general:

- For large companies and enterprises processing a large amount of data, their compliance requirements are relatively high so that the legal risks will increase accordingly. During the preparation of GDPR, the EU had also fully considered the differences between large companies and small and medium enterprises (SMEs) and reached the consensus that large companies shall assume high standard of liability;

- If a company is complained by data subjects, such complaints will also increase the legal risks since the supervisory authority may carry out investigation pursuant to the investigation of data subjects;

- If the company encounter risks of data leakage or data leakage occurs, it may lead to investigation by supervisory authority.

(4) Brexit’s Impact on Chinese Companies

On January 31, 2020, the UK formally left the EU and entered into a one-year transition period. During the transition period, the UK and the EU need to reach a new free trade agreement. Therefore, the UK will still have to implement the rules of the EU during the transition period. According to the Information Rights and Brexit Frequently Asked Questions on Brexit released by the Information Commissioner’s Office (“ICO”), the transition period will last to the end of 2020, during which the UK is still subject to GDPR. After the transition period, GDPR may no longer applicable to UK but all UK enterprises are required to comply with the UK Data Protection Act. Companies that are subject to GDPR in accordance with Article 3 of GDPR shall still comply with all the requirements of GDPR.

Therefore, for Chinese companies providing goods and services to data subjects in the UK, the data processing activities conducted for domestic personal data subjects in the UK shall
still need to fulfill the requirements of the GDPR in the short term. Meanwhile, companies should continue to pay attention to the status of the signature of Agreement between EU and the UK, and to make corresponding adjustments in a timely manner.

7.2 Methods to achieve GDPR Compliance

Achieving GDPR compliance is a systematic process of company rectification, involving different functional departments, including all affected products, and finally falling to implement the organizational and technical measures of the enterprise with implementation. We understand that the GDPR compliance process shall cover “four elements”, and the whole process shall be divided into “three phases”.

The four elements, organization, process, regulations and training, constitute a complete construction of the data protection management (DPM) system for company’s data protection. GDPR Compliance is never a work can be accomplished by sole legal department or IT department. The primary need is the focus from the management. By issuing decision to lower levels of the company, the management grants necessary authorization to the departments which implement compliance (the core of which includes legal and IT departments) so that they can arrange adequate human and financial resources. This is the first step to initiate a compliance project; data processing activities regulated by the GDPR extend to the entire life cycle of data. Therefore, the GDPR compliance is the compliance of the whole process and lifecycle. The data flow shall be pinpointed based on the Data Mapping so as to determine the risk point and compliance point. Data transfer includes not only transfer within an organization, but also transfer outside the organization, such as data processing, sharing and cross-border transfer, etc.; The core of GDPR is the organizational and technical measures of the company. The effectiveness and enforceability of these measures shall be ensured and they shall be implemented through the rules and regulations of the company and standard procedures. These completed rules, regulations and standard procedures must keep up with the current status of the company and be updated in a timely manner. The training on rules and regulations is a necessary stage for the implement of company’s GDPR compliance projects. The training of rules and regulations can inform relevant departments and employees of their responsibilities and requirements, ensure the effect of implementation and cultivate data protection awareness of the company.

Generally, the GDPR compliance process is divided into three stages: gap analysis, risk assessment and compliance suggestions, implementation and optimization of compliance projects.

(1) Step 1: Gap Analysis

In order to evaluate an enterprise’s data protection status, the gap between the current status and the obligations prescribed by GDPR shall be analyzed at first. Gap analysis requires
the collection of relevant information on the compliance status of company with regard to data protection, such as: the data processing department, purpose of processing, categories of data processed, division of internal responsibilities, safeguards measures for the rights of data subjects, the implementation of the data protection officer system, IT security measures, etc. Second, the gap should be evaluated based on the GDPR requirements that are applicable to a specific company.

(2) Step 2: Risk Assessment and Compliance Recommendations

It is not easy to fulfill the requirements of GDPR and it is also difficult to satisfy all the requirements at the same time. Company shall evaluate the degree of risks of various data processing activities on the business of the companies, the rights of data subjects, and the possibility of causing legal risks, reasonably allocate resources, and propose feasible compliance suggestions.

(3) Step 3: Implementation and Optimization of Compliance Projects

The achievement of GDPR compliance needs the cooperation of the European entities of the companies involved and the clear understanding of the management of the enterprise on compliance affairs. If the enterprise has an office or entity in the EU, the company shall assign project duties to the key personnel of the EU office of the company and designate a project manager to direct the project. If there is no such office or entity, it may consider starting with the establishment of a representative as required by GDPR together with other compliance measures.

8. Risks Reflected in GDPR Enforcement Cases

Since GDPR came into effect on May 25, 2018, data protection, data protection authorities of EU member states have continuously strengthened the frequency and intensity of law enforcement. The first anniversary report of GDPR enforcement issued by EDPB\(^2\) on May 22, 2019 shows, by the end of March, 2019, 281,088 enforcement cases had been reported. The cases were mainly divided into three main categories, of which nearly half (144,376) were complaints, nearly one-third (89,271) were data breaches and the rest (47,441) involved other issues. Since the second half of 2019, there have been sky-high-fine cases like British Airways (fined 204 million euros for data breaches) and Marriott Group (fined 110 million euros for data breaches). The number of enforcement cases continues to increase.

To understand the GDPR enforcement and the main focus of enforcement authorities, we select some of the typical enforcement cases to sort out and refine the basic scenarios and provide relevant risk warnings. The scenarios are divided into three categories: (1)
daily activities, that are, inevitable activities in everyday work of company employees; (2) business development activities, including application launch and advertisement and so on; (3) employee management activities, including the personal data processing activities that may be involved when managing employees within the companies. Companies can refer to the following risk tips for self-evaluation and review of data processing activities, and take corresponding measures to prevent and control regulatory compliance risks.

8.1 Daily Activities.

For daily activities, companies should guide employees to accurately identify whether they will involve the processing of personal data and clarify the related requirements that have to comply with, so as to avoid possible non-compliance behaviors of employees.

<table>
<thead>
<tr>
<th>No.</th>
<th>Specific Scenarios</th>
<th>Risk Warning (Points of Punishment)</th>
<th>Representative case</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Document Signature</td>
<td>The agreement was signed in electronic form to collect biometric signature data of personal data subjects.</td>
<td>According to Article 5 of GDPR which stipulates the principles of purpose limitation and data minimisation, the collection of personal data should be limited in the necessary scope in relation to the purpose. In this scenario, the signature can achieve its purpose on a paper-based agreement, and there is no necessity to use the electronic form.</td>
</tr>
<tr>
<td>2</td>
<td>Web Publishing</td>
<td>The news media disclosed the names and photos of police officers when reporting illegal detention cases in the form of electronic and paper-based newspapers.</td>
<td>According to Article 5 of GDPR which stipulates the principles of purpose limitation and data minimisation and Article 6 regarding the basic legal requirements of data processing, in this scenario, the purpose of news reporting can be achieved by referring to the initials of the data subjects’ names or through facial blurring, long-distance shooting, etc., and the above methods will not have a substantial impact on the events in the news report. Directly disclosing the name of police officers lacks corresponding legal basis and is beyond the necessary scope for news reporting.</td>
</tr>
<tr>
<td>No.</td>
<td>Specific Scenarios</td>
<td>Risk Warning (Points of Punishment)</td>
<td>Representative case</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------</td>
<td>-------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>3</td>
<td>Mailing</td>
<td>One person sent an e-mail to multiple people by copying instead of bcc, resulting in everyone seeing other persons’ personal email address, and 1 was later charged with multiple infringements.</td>
<td>According to Article 6 of GDPR, data processing activities should have appropriate legal basis. In this scenario, the disclosure of e-mail addresses to third party does not have corresponding legal basis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Country: Germany</td>
<td>Supervisory Authority: The Federal Commissioner for Data Protection and Freedom of Information (BfDI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Industry: / (Individual)</td>
<td>Fines: 2,000 euros</td>
</tr>
<tr>
<td>4</td>
<td>Paper Documents</td>
<td>Paper documents are kept in cartons without any protective measures, resulting in the breach of personal data contained therein.</td>
<td>According to Article 5 of GDPR regarding the principle of integrity and confidentiality as well as Article 32 concerning the security requirements for personal data, in this scenario, the lack of protective measures over paper documents, resulted in the personal data breach contained therein.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Country: Czech</td>
<td>Supervisory Authority: Úřad pro ochranu osobních údajů (the Office for Personal Data Protection, UOOU)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Industry: Financial Institutions.</td>
<td>Fines: 1,165 euros</td>
</tr>
<tr>
<td>5</td>
<td>Portable Storage</td>
<td>A data controller lost a flash drive containing personal data, causing data breach and failed to notify the supervisory authority within 72 hours.</td>
<td>According to Article 32 &amp;33 of GDPR, the controller shall implement appropriate technical and organizational measures to ensure the security and confidentiality of personal data, and should notify the supervisory authority within 72 hours. In this scenario, the controller did not implement appropriate measures to ensure the safety of portable storage and did not notify the supervisory authority in line with the requirements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Industry: / (Individual)</td>
<td>Fines: 15,150 euros</td>
</tr>
<tr>
<td>6</td>
<td>Video Surveillance</td>
<td>A store installed video surveillance devices in front of the store to monitor the sidewalk and did not clearly label the monitoring area.</td>
<td>According to Article 13 of GDPR, when personal data relating to a data subject are collected from the data subject, the controller shall provide the data subject with relevant information. In this scenario, the store was monitoring the public area but failed to inform the data subjects through methods like labeling the monitoring scope.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Country: Austria</td>
<td>Supervisory Authority: Austrian Data Protection Authority</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Industry: /</td>
<td>Fines: 4,800 euros</td>
</tr>
<tr>
<td>No.</td>
<td>Specific Scenarios</td>
<td>Risk Warning (Points of Punishment)</td>
<td>Representative case</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Security Service</td>
<td>For one thing, According to Article 5 of GDPR regarding the purpose of limitation and data minimisation, in this scenario, measures such as metal detectors or security screening can be used for security purposes without excessive collection of personal data. For another, according to the basic requirements of Article 6, in this scenario, the data processing activities shall be based on the consent of legal subjects. As the data subjects’ refusal to provide relevant information will result in his inability to enter the venue, there is flaw in the consent.</td>
<td>Country: Hungary Supervisory Authority: The National Authority for Data Protection and Freedom of Information (NAIH) Industry: Cultural Entertainment Fines: 92,146 euros</td>
</tr>
<tr>
<td>8</td>
<td>Response to Rights Requests</td>
<td>According to Article 17 of GDPR, the data subject owns the right to erasure, that is, to obtain from the controller the erasure of personal data, and the controller shall have the obligation to erase personal data without undue delay. In this scenario, the controller did not adequately response to the data subject’s requests, violating the rules of GDPR.</td>
<td>Country: Spain Supervisory Authority: Agencia Española de Protección de Datos (AEPD) Industry: Telecommunications Fines: 27,000 euros</td>
</tr>
</tbody>
</table>

**8.2 Business Development Activities**

Business development activities are the activities that companies are most engaged in and therefore most concerned about. When carrying out business development activities, the companies shall, in the light of the specific business conditions control risks and take appropriate organizational and technical measures to ensure the data processing activities are carried out in compliance and the rights of data subject are fully guaranteed.
<table>
<thead>
<tr>
<th>No.</th>
<th>Specific Scenarios</th>
<th>Risk Warning (Points of Punishment)</th>
<th>Representative Cases</th>
</tr>
</thead>
</table>
| 1   | Sending Advertisements                                 | According to Article 21 of GDPR, the data subject shall have the right to object processing personal data for the purpose of direct marketing. In this scenario, data controller did not adequately respond to data subjects’ request for not sending advertisements, violating rules of GDPR. | Country: Germany  
Supervisory Authority:  
The Federal Commissioner for Data Protection and Freedom of Information (BfDI)  
Industry: Takeaway platforms  
Fines: 195,407 euros |
| 3   | Obtaining from Public Channels                        | According to Article 14 of GDPR, when collecting data not directly from data subjects, it is also necessary to provide data subjects with information about data processing activities to meet the requirements of transparency. | Country: Poland  
Supervisory Authority:  
Urząd Ochrony Danych Osobowych (Personal Data Protection Office, UODO)  
Industry: Internet (digital marketing)  
Fines: 219,538 euros (*The final fine is under review) |
| 4   | Supplier Management                                   | According to Article 28 of GDPR, the processing behavior of data processors should be subject to contract law or relevant provisions. In this scenario, the data controller designated a third-party supplier to process customer data without signing a data processing agreement, and transmitted the data to the supplier for processing without knowing the data processing process of the supplier, which violates GDPR. | Country: Germany  
Supervisory Authority:  
The Federal Commissioner for Data Protection and Freedom of Information (BfDI)  
Industry: Internet  
Fines: 5,000 euros |
<table>
<thead>
<tr>
<th>No.</th>
<th>Specific Scenarios</th>
<th>Risk Warning (Points of Punishment)</th>
<th>Representative Cases</th>
</tr>
</thead>
</table>
| 5   | Acquisition Investment                   | According to Article 32 of GDPR, appropriate technical and organizational measures shall be implemented to protect personal data security, to avoid illegal destruction, loss, tampering, unauthorized disclosure or access of personal data. In the scenario, during the acquisition of investment, insufficient due diligence was conducted to find the existing system vulnerabilities, and appropriate technical and organizational measures were lacked. | Country: the UK Supervisory Authority: Information Commissioner’s Officer (ICO)  
Industry: Hotels (Marriott Hotel)  
Fines: 110 million euros |
| 6   | Applications                             | According to Article 32 of GDPR, appropriate technical and organizational measures shall be implemented to protect personal data security. In this scenario, the application was not properly tested before it was put into use, and the security vulnerabilities were not found, violating the rules of GDPR. | Country: Norway Supervisory Authority: The Norwegian Data Protection Authority  
Industry: Administration  
Fines: 203,000 euros |

8.3 Employee Management Activities

For the personal data processing activities that occur in the process of employee management, the particularity of the relationship between the company and the employees should be fully considered when demonstrating the legal basis of the data processing activities and processing personal data of the employees, so as to avoid inappropriate measures due to inequality between the two parties.
<table>
<thead>
<tr>
<th>No.</th>
<th>Specific Scenarios</th>
<th>Risk Warning (Points of Punishment)</th>
<th>Representative Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Employee manage- ment</td>
<td>When processing the personal data, the controller took the consent of data subjects to serve as the legal basis.</td>
<td>According to Article 6 of GDPR, data processing activities shall have appropriate legal basis. Due to the inequality between the company and employees, such consent cannot be deemed to be based on the free will of employees, and does not constitute an effective consent to meet the GDPR requirements.</td>
</tr>
<tr>
<td>2</td>
<td>Information Disclosure</td>
<td>When disclosing information about internal personnel on the public web beyond the necessary scope, there may be a risk of unauthorized use of the disclosed personal data.</td>
<td>According to Article 5 regarding the principles of purpose limitation and data minimisation, the use of personal data should be seriously limited to the necessary scope in relation to the purpose. In this scenario, disclosing employees’ information is beyond the necessary minimum scope.</td>
</tr>
<tr>
<td>3</td>
<td>Video Surveillance</td>
<td>To ensure the safety of personnel and property, the company installs video surveillance equipment to continuously monitor employees.</td>
<td>In one hand, according to the principles of purpose limitation and data minimisation in Article 5 of GDPR, in this scenario, continuous and permanent monitoring can be carried out by adjusting the installation position, direction and operation period of the monitoring equipment. In another hand, according to the legal basis requirement in Article 6 of GDPR, the installation of video surveillance equipment in the workplace must have a specific and clear purpose and appropriate legal basis.</td>
</tr>
<tr>
<td>No.</td>
<td>Specific Scenarios</td>
<td>Risk Warning (Points of Punishment)</td>
<td>Representative Cases</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 4   | Face Recognition              | Face recognition technology was used for checking work attendance, and the consent of the data subject serves as the legal basis for this data processing activity. At the same time, the data protection impact assessment was not conducted before the face recognition was put into use, and there was no communication with local data protection supervisory authority.  
For one thing, according to Article 6 of GDPR, data processing activities shall have appropriate legal basis. Due to the inequality between the company and employees, such consent cannot be deemed to be based on the free will of employees, and does not constitute an effective consent to meet the GDPR requirements.  
For another thing, according to Article 35 of GDPR, the controller shall carry out data protection impact assessment in special situations and actively communicate with data protection authorities. | Country: Sweden  
Supervisory Authority: The Swedish Data Protection Authority  
Industry: Education  
Fines: 18,630 euros |

Based on the above-mentioned representative cases and risk warning, in order to actively respond to the complaints of data subjects and the review of supervisory authorities, the company should set up compliance regulations and embed the regulations in the business process in line with the requirements of law and industry practices. It is recommended to pay attention to the following issues: strengthen the security safeguard of personal data to avoid the illegal access, use and accidental disclosure, damage, and loss of personal data; attach importance to the data subject’s right request, and respond positively and effectively to reduce complaints from the data subject; carry out adequate risk assessment for new business and activities, and take timely risk response measures; strengthen employee training and improve overall compliance awareness.
PART II

How Chinese Companies Comply with GDPR Compliance

1. Tendency: Progress in the Interpretation of GDPR

As a comprehensive and systematic data protection regulation, GDPR is quite complex. To further clarify the important contents, the European Data Protection Board (EDPB), an independent institution established in accordance with GDPR, issues detailed guidelines for the interpretation on key themes. Besides, when GDPR came into effect, EDPB also stated that it will endorse guidance documents issued by WP29 (Article 29 Working Party, established in accordance with EU Data Protection Directive) on the premise that they will not affect any subsequent appropriate amendments. By now, EDPB and WP29 have published 31 guidelines in total, which gradually forming a GDPR regulation system with laws as principles and guidelines as supplements.

The following form aims at showing the tendency of GDPR clearly and intuitively. In the form, the key themes and main contents are sorted out in the order of time. With the advancement of GDPR practice and the rapid change of personal data processing technology, EDPB may issue other guidelines to further improve and optimize GDPR regulation system.
<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Theme</th>
<th>Release Date</th>
<th>Revision Date</th>
<th>Main Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Guidelines 05/2020 on consent under Regulation 2016/679</td>
<td>Consent</td>
<td>20200504</td>
<td>/</td>
<td>The Guideline further clarifies the requirement for valid consent, the requirement for valid explicit consent and the distinction between consent and other legal basis, on the basis of the WP29 Guidelines.</td>
</tr>
<tr>
<td>2</td>
<td>Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak</td>
<td>Legitimate Use</td>
<td>20200416</td>
<td>/</td>
<td>The Guideline deals with the basic requirements to trace Apps during the COVID-19 outbreak: resources, approval of national health authority, timely deletion of related data.</td>
</tr>
<tr>
<td>3</td>
<td>Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak</td>
<td>Legitimate Use</td>
<td>20200421</td>
<td>/</td>
<td>The Guideline deals with the legal basis for processing data concerning health for the purpose of scientific research, the needed safeguards, and the exercise of rights of data subjects during the COVID-10 outbreak. Scientific research does not take precedence over the basic rights and freedom of data subject, and a balance shall be established. The Guidelines also allow EU members to make detailed regulations.</td>
</tr>
<tr>
<td>4</td>
<td>Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies - version for public consultation</td>
<td>Cross-border Transfers</td>
<td>20200224</td>
<td>/</td>
<td>The Guideline deals with the personal data transfer between public authorities of European economic areas and non-European economic areas. The international agreement signed by public authorities shall incorporate minimum safeguards, in line with basic principles like purpose limitation, data minimization. Storage limitation and so forth, ensuring the safety and confidentiality of data as well as the realization of data subject rights.</td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Theme</td>
<td>Release Date</td>
<td>Revision Date</td>
<td>Main Contents</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------</td>
<td>--------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>5</td>
<td>Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications - version for public consultation</td>
<td>Connected Vehicles and Mobility</td>
<td>20200207</td>
<td>/</td>
<td>The Guideline deals with the personal data process during the processing of vehicles, personal data connected to exchange equipment between the vehicle and individuals (such as smartphones) and summarizes the risks that processing activities may face. As the information is asymmetric and personal data subjects lack control over its data, the user consent is difficult to obtain, and the quality is hard to guarantee, and the data is too much to collect. Therefore, vehicle and device manufactures, service providers or others who may constitute data controllers or processors should classify data restrict the purpose of use, ensure relevance and data minimization, pay attention to the realization of PbD, notify timely, use security technology, adopting in-car WiFi technology to control risks.</td>
</tr>
<tr>
<td>6</td>
<td>Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under GDPR (part 1) - version for public consultation</td>
<td>The Rights of Data Subjects</td>
<td>20191211</td>
<td>/</td>
<td>The Guideline clarifies the following important contents: (1) the data subject can make a request for the right to be forgotten against website containing his personal data; (2) the search engine operators can refuse such request in certain exceptional situations.</td>
</tr>
<tr>
<td>7</td>
<td>Guidelines 4/2019 on Article 25 Data Protection by Design and by Default - version for public consultation</td>
<td>DPbDD</td>
<td>20191113</td>
<td>/</td>
<td>The Guideline further clarifies the content and practical requirements of Article 25 of GDPR, including the scope of application, analysis of the provisions, how to implement the basic principles of data protection through DPbDD, certification, implementation and recommendation.</td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Theme</td>
<td>Release Date</td>
<td>Revision Date</td>
<td>Main Contents</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>8</td>
<td>Guidelines 3/2019 on processing of personal data through video devices - version for public consultation</td>
<td>Special Processing (video devices)</td>
<td>20190712</td>
<td>/</td>
<td>The Guideline aims to provide basic guidance on how to apply GDPR to all personal areas of video device application. It clarifies the scope of application, the legal basis for processing activities, the requirements for purpose limitations, the requirements for processing special categories of personal data, transparency requirements, data storage deadlines and security assurance requirements.</td>
</tr>
<tr>
<td>9</td>
<td>Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725)</td>
<td>Administration (Official Authorities)</td>
<td>20190710</td>
<td>/</td>
<td>Regulation (EU) 2018/1725 (Regulation on the protection of natural persons with regard to the processing of personal data by Union institutions) came into effect on December 11, 2018, regulating the protection of data and the free flows of data by EU authorities in processing of personal data. The EU authorities in the regulation are not subject to GDPR. EDPB proposes amendments to Article 38.4 of the above regulation through the Guidelines.</td>
</tr>
<tr>
<td>10</td>
<td>Guidelines 2/2019 on the processing of personal data under Article 6(1) (b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation</td>
<td>Legal Basis</td>
<td>20190409</td>
<td>20191008</td>
<td>The Guideline clarifies the situations in which data processing activities in scenarios of providing online services can be based on the legal basis necessary to perform a contract, factors that need to be considered when judging whether it constitutes necessity, and typical scenarios where the legal basis for performing the contract is liable to be incorrectly applied.</td>
</tr>
<tr>
<td>11</td>
<td>EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation</td>
<td>Administration (Supervisory Authority)</td>
<td>20190212</td>
<td>20190604</td>
<td>According to Article 40 &amp; 41 of GDPR, EU member states and supervisory authorities can make codes of conduct to promote the application of GDPR according to specific needs. The Guideline aims to explain and clarify article 40 &amp; 41 of GDPR, and clarify the basic framework and necessary elements of the code of conduct.</td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>DPB Guidelines 3/2018 on the territorial scope of GDPR (Article 3) - version adopted after public consultation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Theme</th>
<th>Release Date</th>
<th>Revision Date</th>
<th>Main Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification</td>
<td>20180206</td>
<td>20181204</td>
<td>20190604</td>
</tr>
<tr>
<td>Territorial Scope</td>
<td>20191116</td>
<td>20191112</td>
<td>As one of the most important Guidelines issued by EDPB, the Guideline aims to provide basic instruction for judging the jurisdiction of GDPR. According to Article 3 of GDPR and the Guidelines, judgement can be made on the basis of two criteria: establishment and targeting. GDPR is applicable to data processing activities carried out in business premises within the EU, even if no business premises are established within the EU, in case providing products or services to data subjects within EU or monitoring the data subjects within the EU, relevant behavior is subject to GDPR.</td>
</tr>
<tr>
<td>Cross-border Transfers</td>
<td>20190525</td>
<td>/</td>
<td>According to Chapter 5 of GDPR, the cross-border data transmission must have a corresponding transmission guarantee mechanism. Meanwhile, the Guideline provides a detailed analysis of the specific situations, and clarifies the criteria for the application of the derogations.</td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Theme</td>
<td>Release Date</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------</td>
<td>--------------</td>
</tr>
<tr>
<td>15</td>
<td>EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation</td>
<td>Certification</td>
<td>20180525</td>
</tr>
</tbody>
</table>

**WP29 Guidelines recognized by EDPB**

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Theme</th>
<th>Release Date</th>
<th>Revision Date</th>
<th>Main Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Guidelines on consent under Regulation 2016/679, WP259 rev.01</td>
<td>Legal Basis</td>
<td>20171128</td>
<td>20180410</td>
<td>The consent of the data subject is one of the common legal basis of data processing activities, and some misunderstandings will inevitably occur in practice. The Guideline clarifies the constituent requirements of effective consent under GDPR: freely given, specific, informed and unambiguous indication of the data subject's wishes, and provides a clearer guidance of how to obtain effective consent of the data subject.</td>
</tr>
<tr>
<td>17</td>
<td>Guidelines on transparency under Regulation 2016/679, WP260 rev.01</td>
<td>Transparency</td>
<td>20171129</td>
<td>20180411</td>
<td>The Guideline aims to provide basic guidance on how to meet the transparency requirements of GDPR by explaining the implementation elements of transparency (clear, specific, easy to access, free and so forth) and specific requirements for providing data to the data subject information requirements and descriptions in the form of examples as the basic guidance for companies to make privacy policies.</td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Theme</td>
<td>Release Date</td>
<td>Revision Date</td>
<td>Main Contents</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>18</td>
<td>Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01</td>
<td>Special Processing (Automated Individual Decision-making and Profiling)</td>
<td>20171003</td>
<td>20180206</td>
<td>Considering the significant risks that automated decision-making and profiling may pose to data subjects’ rights and freedom, GDPR provides special requirements for data subject protection for such behaviors. To further clarify relevant requirements of GDPR, the Guideline explains the definition of automated decision-making and profiling, and analyzed the special requirements for such processing behaviors in detail based on Article 22 of GDPR, and provide guidance on regulatory compliance for automated decision-making and profiling technology.</td>
</tr>
<tr>
<td>19</td>
<td>Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01</td>
<td>Personal Data Breach</td>
<td>20171003</td>
<td>20180206</td>
<td>According to Article 33 &amp; 34, in the case of a personal data breach, the controller shall notify Supervisory Authority in time, and when being likely to result in a high risk to the rights and freedoms of the data subject, the subject should also be notified. The Guideline aims at explaining the possible serious result of personal data breach, when to notify, serving as a fundamental guidance for positively and appropriately tackling personal data breach.</td>
</tr>
<tr>
<td>20</td>
<td>Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01</td>
<td>Rights of the Data Subject</td>
<td>20161213</td>
<td>20170405</td>
<td>According to Article 20 of GDPR, the data subject shall have the right to data portability, namely, to receive the personal data from a controller and transmit those data to another controller. The guideline aims to further clarify the requirements, the realization and the application scope of right to portability, provide detailed advice for enterprises to use technology method to realize the right.</td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Theme</td>
<td>Release Date</td>
<td>Revision Date</td>
<td>Main Contents</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------</td>
<td>--------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>21</td>
<td>Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP248 rev.01</td>
<td>DPIA</td>
<td>20170404</td>
<td>20171004</td>
<td>According to Article 35 of GDPR, when the data processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out assessment of the impact of the envisaged processing operations on the protection of personal data. The Guideline aims to further clarify how to judge the high risk a processing can cause, and provide fundamental guidance on the requirements and procedures for impact assessment.</td>
</tr>
<tr>
<td>22</td>
<td>Guidelines on Data Protection Officers (‘DPO’), WP243 rev.01</td>
<td>DPO</td>
<td>20161213</td>
<td>20170405</td>
<td>According to Article 37 of GDPR, the controller and the processor shall designate a data protection officer. The Guideline aims to further clarify basic issues like under which situation the data protection officer should shall be designated, what status the data protection officer enjoys and what responsibilities a data protection officer should assume. The Guidelines explain these issues in detail.</td>
</tr>
<tr>
<td>23</td>
<td>Guidelines for identifying a controller or processor’s lead supervisory authority, WP244 rev.01</td>
<td>Administration (Supervisory Authorities)</td>
<td>20161213</td>
<td>20170405</td>
<td>The Guideline clarifies the important concepts and steps for identifying a controller or processor’s lead supervisory authority, and provide basic guidance on how to identify lead supervisory authority in two special situations (cross-border data transmission, data controllers and processors established outside the EU).</td>
</tr>
<tr>
<td>24</td>
<td>Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR</td>
<td>Records of Processing Activities</td>
<td>20180419</td>
<td>/</td>
<td>Article 30 of GDPR stipulates that the controller and processor shall maintain a record of processing activities under its responsibility and special situations which can derogate the responsibility. The Guideline also shows the basic position of WP29 on reducing the responsibility on records of processing activities, encourage the supervisory authorities of EU member states to support SMEs by providing tools that facilitate the establishment and management of records.</td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Theme</td>
<td>Release Date</td>
<td>Revision Date</td>
<td>Main Contents</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>25</td>
<td>Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under GDPR, WP 263 rev.01</td>
<td>Cross-border Data Transfers</td>
<td>20180411</td>
<td>/</td>
<td>According to Chapter 5 of GDPR, cross-border data transmission must be carried out under an appropriate safeguard mechanism. Article 47 stipulates one of them, binding corporate rules. If the rules are legally binding, they apply to all relevant members of the enterprise group, and provide the data subjects enforceable rights. The rules shall also clarify the contents of GDPR. WP29 has issued a series of working documents, recommendation documents, etc., which clarify what elements should be included in the binding corporate rules, what principles should be followed, how to apply and how to approve the supervisory authorities, which are the fundamental practical basis for establishing binding corporate rules.</td>
</tr>
<tr>
<td>26</td>
<td>Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264</td>
<td>Cross-border Data Transfers</td>
<td>20180411</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265</td>
<td>Cross-border Data Transfers</td>
<td>20180411</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01</td>
<td>Cross-border Data Transfers</td>
<td>20180206</td>
<td>20181128</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01</td>
<td>Cross-border Data Transfers</td>
<td>20180206</td>
<td>20181128</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Adequacy Referential, WP 254 rev.01</td>
<td>Cross-border Data Transfers</td>
<td>20171128</td>
<td>20180206</td>
<td>WP29 published the documents to update the content of WP12 (Working Document on transfer of personal data to third countries) issued on July 24, 1998, and supplement the identification elements for adequacy decision, the procedures and other contents.</td>
</tr>
</tbody>
</table>
2. Under Which Circumstances Will GDPR be Applied out of EU?

——An Interpretation on EDPB Guidelines on the territorial scope of the GDPR (Article 3)

Preamble

The extraterritorial effectiveness of GDPR is one of the important reasons why industries in the world concern about GDPR. Chinese companies may also fall in the jurisdiction scope of GDPR when carrying out data processing activities. For companies, the first step to carry out data compliance work is determining whether GDPR is applicable to the personal data processing activities.

According to Article 2 and Article 3 of GDPR, when determining whether the data processing activities fall within the scope of GDPR, the companies should consider the requirements of material scope and territorial scope. As for the material scope, GDPR only applies to personal data processing activities. If the data processing activity of a company does not involve personal data, it will not fall within application scope of GDPR. Compared to the determination of material scope, the determination of territorial scope is more complicated.

To better guide companies to determine whether the corresponding personal data processing activities fall within the scope of GDPR, EDPB, on the basis of version for public consultation, officially issued Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version 2.0 \(^3\) (hereinafter referred to as the “Guidelines”) on November 12, 2019.

According to Article 3 of GDPR and the Guidelines, determining the territorial scope of GDPR should follow the following three criteria: the establishment criterion, targeting criterion and the application of relevant international law. We will focus on the interpretation of establishment criterion and targeting criterion in the following.

---

\(^3\) [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en, the last visit: June 10, 2020.](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en, the last visit: June 10, 2020.)
2.1 Establishment Criterion

Article 3(1) of GDPR: This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

(1) the Judgement of Establishment

According to Recital 22, establishment implies the effective and real exercise of activities through stable arrangements. Therefore, the core of determining whether a data controller or processor has an establishment in the EU, is to judge the degree of stability of the arrangements based on the nature of the provided services and the effective exercise of activities in the EU.

The scope of establishments is quite wide. Hence, stable arrangement does not mean the company must have a branch or subsidiary with a legal personality in the EU. In some circumstances, the presence of one single employee or agent of the data controller or processor may be sufficient to constitute a stable arrangement, if that employee or agent acts with a sufficient degree of stability. Accordingly, the effective and real exercise of activities of the data controller or processor through this stable arrangement can be deemed as an establishment in EU. It should be noted that the scope of establishments is not without limits. It is not possible to conclude that the non-EU entity has an establishment in the Union merely because the undertaking’s website is accessible in the Union.

(2) Application of Establishment Criterion

A. Personal Data Processing Activities in the Context of the Activities of an Establishment

The application of establishment criterion requires the personal data processing activities by a personal data controller or processor are carried out in the context of the activities of its relevant EU establishments. The Guidelines point out that, for non-EU data controllers and processors, determining whether personal data processing activities are carried out in the context of the activities of its relevant EU establishments is made on a case-by-case basis. In the analysis, the following two factors should be taken into account:

(i) Does the data controller and processor outside the EU have an inextricably link with of a local establishment in the EU? If such link exists, even if the local establishment is not actually taking any role in data processing itself, the data processing activities by the data controller or processor of shall be governed by GDPR;

---

4 Recital 22. Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.
(ii) Does the data controller and processor outside the EU have revenue raising in the EU by a local establishment? If the establishment in the EU conducts revenue activities, and the revenue is inextricably linked to the processing of personal data being place outside the EU by the data controller or processor, the data processing activities by the data controller or processor of shall be governed by GDPR.

B. Regardless of Whether the Processing Takes Place in the EU

When applying the establishment criterion, the geographical location of the data processing activities by the data controller or processor is not a consideration. Even if the processing does not take place in the EU, GDPR shall still apply if personal data processing activities by a personal data controller or processor are carried out in the context of the activities of its relevant EU establishments.

(3) Application of Establishment Criterion to Controllers and Processors

According to Article 3(1) of GDPR, controllers and processors can determine whether the personal data processing activities fall within the scope of GDPR by applying the establishment criterion. The Guidelines highlight that the existence of a relationship between a controller and a processor does not necessarily trigger the application of GDPR to both, should one of these two entities not be established in EU.

A. Processing by a Controller in the EU Using a Processor outside the EU

Where a controller subject to GDPR chooses to use a processor located not subject to the GDPR, it will be necessary for the controller to ensure by contract or other legal acts that the processor processes the data in accordance with article 28 of GDPR. The controller needs to ensure the processor addressing all the requirements in line with GDPR and the controller’s instruments. Therefore, the processor not subject to the GDPR will become indirectly subject to some obligations imposed by controllers subject to the GDPR by virtue of contractual arrangements under Article 28.

B. Processing by a Controller outside the EU Using a Processor in the EU

Data controllers established outside the EU will not be subject to GDPR simply by instructing data processors in the EU to conduct personal data processing activities. In this scenario, the processing is carried out in the context of the controller’s own activities; the processor is merely providing a processing service, which is not inextricably linked to the activities of the controller.

2.2 Targeting Criterion
Article 3(2) of GDPR: This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

The absence of an establishment in the EU does not necessarily mean that a data controller or processor established would be excluded from the scope of the GDPR. If the data controller or processor is involved in two specific types of personal data processing activities related to the personal data subjects in the EU, it may still be regulated by GDPR.

(1) Offering of Goods or Services to Data Subjects in the EU

Determining whether it constitutes the offering of products or services to personal data subjects in the EU does not depend on whether payment is made in exchange for the goods or services provided. Besides, data controllers or processors should offer products or services to personal data subjects intentionally, not unintendedly or accidentally. According to the Guidelines, the data controller or processor should at least fully consider the following factors when determining:

(i) The EU or at least one Member State is designated by name with reference to the good or service offered;

(ii) The controller or processor has launched marketing and advertisement campaigns directed at an EU country audience;

(iii) The mention of dedicated addresses or phone numbers to be reached from an EU country;

(iv) The use of a top-level domain name of the EU or one of the Member States, for example “.de” or “.eu”;

(v) The use of a language or a currency of one or more EU Member States.

(2) Monitoring of Data Subjects’ Behaviour

To determine whether article 3(2)(b) of GDPR apply, the behavior monitored by the data controller or processor must be related to the personal data subject in the EU, and the monitored behavior must take place within the EU. The two criteria must be met.

Recital 24 states that “in order to determine whether a processing activity can be considered
to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.\(^5\) Accordingly, the Guidelines emphasize that the use of the word “monitoring” implies that the data controller or processor has a specific purpose in mind for the collection, which is the subsequent reuse of the relevant data about an individual's behaviour within the EU. Typical monitoring activities include behavioural advertisement, online tracking through the use of cookies or other tracking techniques such as fingerprinting, market surveys and other behavioural studies based on individual profiles.

(3) Application of Targeting Criterion to Controllers and Processors

Since only the data controller has the right to determine the purpose and method of personal data processing activities, in principle, it is mainly for the data controller to judge whether the personal data processing activities it carries out are subject to GDPR by applying the targeting criterion in Article 3(2) of GDPR.

For the data processor established outside the EU, the key to determining whether it is subject to GDPR under the targeting criterion is to assess whether the personal data processing activities undertaken by the data processor are related to the data controller's target activities. If the personal data processing activities carried out by the data processor in accordance with the data controller’s instructions are related to the data controller’s target activities for personal data subjects in the EU, the personal data processing activities carried out by the data processor are subject to GDPR.

Conclusion

For companies outside the EU, determining whether GDPR shall apply is the starting point and basis for GDPR compliance. When Chinese companies expand the EU market, they may set up local branches, representatives, offices, etc., or directly provide products or services to local users. At the same time, more and more companies are working as data processors with local companies in the EU to conduct business. The Guidelines provide clear guidance for companies to determine whether their personal data processing activities are subject to GDPR. Companies can make judgments accordingly and carry out compliance work in conjunction with other GDPR requirements.

\(^5\) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.
3. What is Valid Consent under GDPR

——An Interpretation on EDPB’s Guidelines 05/2020 on consent under Regulation 2016/679

Preamble

According to Article 6 of GDPR, there shall be appropriate legal basis for the processing of personal data. For common companies, the most commonly used legal basis include the consent of data subjects, necessary for the performance of a contract and legitimate interest. Particularly, the consent of data subjects is recognized as the most important legal basis for the legal and justifiable processing of personal data by various states and organizations. In China, according to the provisions of CSL, any collection and use on personal information shall be subject to the consent of subjects concerned.6

On April 10, 2018, Working Party 29 has passed Article 29 Working Party Guidelines on consent under Regulation 2016/679. EDPB updated and revised based on the guidelines and issued Guidelines 05/2020 on consent under Regulation 2016/6797 on May 5, 2020 (hereinafter referred to as “the Guidelines”). In the Guidelines, EDPB has specified the method to obtain valid consent of data subjects in detail.

3.1 What is a valid consent?

According to the definition of consent in Article 4 of GDPR and conditions for consent in Article 7, the elements for a valid consent are: freely given; specific; informed; unambiguous indication of wishes; the possibility to withdraw consent at any time. Meanwhile, data controllers shall be able to demonstrate that the data subject has given his/her consent to the processing of his/her personal data.

(1) Freely given

The element “free” means the data subjects are compelled to consent. Also, data subjects is able to refuse or withdraw his or her consent without detriment. Any consent obtained by inappropriate pressure or influence upon the data subject or by force shall not constitute a valid consent. To ensure the consent of data subjects are freely given, the following questions should be taken into consideration:

First, data controllers shall fully consider the imbalance of the relationship between data controller and data subjects. A typical example of imbalance of power occurs in the employment context. Given the dependency that results from the employer/employee

---

6 Article 41 of Cyber Security Law of People’s Republic of China: To collect and use personal information, network operators shall follow the principles of legality, rightfulness and necessity, disclose the rules for collection and use, explicitly indicate the purposes, means and scope of collecting and using information, and obtain the consent of the persons whose information is collected.

relationship, it is unlikely that the data subject is able to refuse to give consent for the data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. Therefore, for the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees\(^8\).

Second, data controllers shall avoid bundling the consent to acceptance of terms or conditions, which may cause confusion to data subjects. The consent of data subjects and necessity for the performance of a contract is two independent legal basis for the processing of personal data and shall not be combined and confused. Therefore, “necessary for the performance of a contract” must be interpreted strictly. The assessment of necessity requires that there should be a direct and objective relation\(^9\) between the processing of data and the purposes of performing contracts.

Third, data controllers shall fully consider the granularity of the consent. According to Recital 32, when there are multiple purposes of the processing, consent should be given for every purpose. In practice, provision of a service usually involves multiple processing. Under this circumstance, data controllers shall separate the purposes and determine specific legal basis for each purpose. If the processing requires consent of data subjects, the consent shall be obtained for each specific purpose.

Furthermore, the data subjects should have the right to withdraw his/her consent without detriment. If the data controllers can demonstrate that the data subjects may withdraw his or her consent without detriment (e.g. without compromising the quality of service or damaging the data subjects), it is sufficient to demonstrate that the consent of data subjects are freely given.

**(2) Specific**

Specific means the consent of the data subjects shall not be general. The consent of the data subject must be given in relation to “one or more specific” purposes and that a data subject can choose every single one from them. To obtain valid consent of data subjects, the measures taken by the data controllers shall comply with following conditions:

First, data controllers shall specify the purposes in avoid of function creep, that is gradual widening or blurring of purposes for which data is processed, after a data subject has consented to the initial collection of his/her personal data. If a controller processes data

---

8. In July 2019 Hellenic Data Protection Authority (HDPA) imposed a EUR 150,000 penalty on PWC. The HDPA believes that it is not appropriate for PWC to use consent as the legal basis for processing the employee’s personal data because rights between the parties are not equal and an employee’s consent under the employment relationship cannot be considered to have been made voluntarily.

9. According to Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (version for public consultation) issued by EDPB on April 9, 2019, the following issues shall be considered in the assessment of necessity: What is the nature of the service being provided to the data subjects? What is the specific purpose of the contract? What are the mutual perspectives and expectations of the parties to the contract? Would an average user of the service reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract to which they are a party?
based on consent and wishes to process the data for another purpose, the controller needs to seek additional consent for this other purpose unless there is another appropriate lawful basis.

In addition, data controllers shall specify the granularity in consent requests. A controller that seeks consent for various purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes.\(^\text{10}\)

Lastly, the data controllers shall distinguish the information relevant to obtaining consent from other information. The data controllers shall also provide the data subjects with details of the personal data need to be processed for specific purpose in each separate consent request.

(3) Informed

The requirement that consent must be informed means that the consent of data subjects is not made without knowledge of the relevant circumstances in which his/her personal data is processed. The consent obtained by the data controllers will be invalid if the data subject does not understand what they are agreeing to and the rights they have.

At least the following information is required for obtaining valid consent: the controller’s identity; the purpose of each of the processing operations for which consent is sought; what (type of) data will be collected and used; the right to withdraw consent; information about the use of the data for automated decision-making, and the possible risks of data transfers and other information that is vital for data subjects to make a choice.

When seeking for data subjects’ consent, controllers should ensure that they use clear and plain language and provide aforementioned information in a concise way. Obscure and lengthy documents shall be avoided.

(4) Unambiguous indication of wishes

Unambiguous indication of wishes means the consent of data subjects must be given by an active motion or declaration. To obtain unambiguous indication of wishes, the data controller must equip appropriate mechanism to ensure data subjects have taken a deliberate action to consent to particular processing. To obtain unambiguous indication of wishes of data subjects, the following questions can be of guidance:

First, the data controller shall not use pre-ticked opt-in boxes. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as

---

\(^\text{10}\) In January 2019, the Commission Nationale de l’Information et des Libertés (CNIL) imposed a penalty of 50 million euros on Google. One of the claimed violation is that Google requires users to fully agree with the terms and conditions on data processing in its privacy policy, without distinguishing various purposes.
an active indication of choice. Only affirmative act or statement can constitute unambiguous indication of wishes;

Second, the data controller shall not obtain consent through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data;

Third, when consent is to be given following a request by electronic means, the data controller shall manage the subtle balance between obtaining consent and ensuring the validity of the consent. The request for consent should not be unnecessarily disruptive to the use of the service for which the consent is provided.

Lastly, the data controller must ensure that consent always be obtained before the controller starts processing personal data for which consent is needed. If there is a change of the purposes for data processing after consent was obtained or if an additional purpose is envisaged, the data controller shall obtain a new and specific consent.

(5) Withdrawal of consent

According to the requirement of GDPR, a valid consent must ensure that data subjects are able to withdraw consent as easily as it was given at any time.

For one thing, the data controller must ensure the means for withdrawing consent provided to data subjects are easy to operate and the withdrawal of consent will not reduce the service level provided.

For another, under scenarios where consent serves as legal basis, the data controller have the obligation to delete data that was processed on the basis of consent once that consent is withdrawn, assuming that there is no other purpose justifying the continued retention\(^{11}\). If continued processing of data is needed, the data controller is obliged to assess whether continued processing of the data in question is appropriate, even in the absence of an erasure request by the data subject.

(6) Controllers’ obligation to demonstrate the consent

Under the scenario where consent is the basis for data processing, the data controller shall demonstrate that it has obtained valid consent. GDPR does not specify the manner of demonstration and the duration of the consent. EDPB recommends that the data controllers, on the one hand, may retain the consent statement it receives to show how and when

\(^{11}\) In 2018, the Office for Personal Data Protection (OPDP) imposed penalties on a food dealer. One of the claimed violations is the customers of the food distributors complain to OPDP that they have refused or withdrawn the consent to their personal data processing but still receive the contact information of the business, which impairs the legitimate rights and interests of the data subjects.
consent is obtained and the information it provides to the data person; and on the other hand, it should update the consent at an appropriate interval to provide relevant information to the data subjects.

3.2 What is an explicit consent?

Explicit consent is required in certain situations where there are serious data protection risk. According to GDPR, explicit consent mainly apply to the following scenarios:

1. the processing of special categories of data specified in Article 9 of GDPR and Recital 51.

2. automated individual decision-making, including profiling specified in Article 22 of GDPR and Recital 71.

3. derogation for specific situations of data transfers specified in Article 49 of GDPR and Recital 111.\(^{13}\)

EDPB hold the opinion that the term “explicit” refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. Therefore, to obtain explicit consent, the data controller shall fulfill the following requirements:

First, all requirements for consent shall be fulfilled (above-mentioned six specified elements);

Second, data subjects shall make explicit consent in written or oral statements. The statement affirming consent may be conducted either in written form or electronic form, such as by filling electronic forms, sending an email or using an electronic signature.

It is worthwhile to note that, pursuant to the GDPR Guidance published by the Information Commission’s Office (ICO), explicit consent does not require data subjects to prepare a statement of consent by itself. Such statement can be prepared by data controllers in advance provided that data subjects clearly knows the content of the statement and he or she has consented such statement (by signature or voluntarily ticking). Explicit consents may also be given orally, if there is sound recordings or written records. In terms of substance,
there is no substantive difference between consent and explicit consent under GDPR.

### 3.3 How to Distinguish Consent from Other Legal Basis

According to GDPR, a controller needs to identify the appropriate legal basis for the personal data processing activity before conducting and there shall be only one legal basis.

The assessment of the legal basis is closely related to the purpose of data processing. Under scenarios where consent is the legal basis for the data processing, data controllers shall stop relevant processing activities immediately after data subject withdraw his/her consent. Meanwhile, the data controller cannot change one legal basis to other legal basis arbitrarily. For example, when data subjects use consent as legal basis for processing and there is defect in the validity of consent, data controllers may not retrospectively utilize legitimate interests as a legal basis to justify the legality of their data processing.

**Conclusion**

Compared with requirement for consent in CSL and other laws, regulations and national standards, GDPR provides more specified and stricter requirements for consent. Under the framework of CSL, consent is recognized as a general legal basis for processing of personal information in most cases. Only in certain exceptional circumstances, data controllers shall obtain explicit consent of personal information subjects as prerequisite for processing.\(^\text{15}\)

For the time being, there is no systematic regulation corresponding to GDPR’s provisions on consent.\(^\text{16}\) With the enforcement conducted by authorities, the requirements on the validity of consent and explicit consent of personal information subjects have been specified under the context of intensified surveillance and administration.

### 4. What is “Necessary for the Performance of a Contract” under GDPR

—An Interpretation on EDPB Guidelines 2-2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects

**Preamble**

According to Article 6 of GDPR, there shall be appropriate legal basis for the processing of personal data. For common companies, the most commonly used legal basis include the

---

\(^\text{15}\) According to Information Security Technology - Personal Information Security Specification, the circumstances where the explicit consent of personal information subjects is required mainly include: processing the personal information of a special subjects- minors; processing of special types of personal information -the personal sensitive information; conducting special activities (use beyond the scope, etc.).

“Explicit consent” refers to personal information subjects voluntarily makes written or electronic statement through written, oral or other means, or independently makes affirmative action and authorize specific processing of his personal information.

\(^\text{16}\) Information Security Technology - Personal Information Security Specification has proposed requirements for mobile Internet application operators to distinguish the basic business functions from the expanded business functions and obtain the expressed consent from the personal information subjects.
consent of data subjects, necessary for the performance of a contract and legitimate interest.

“Necessary for the performance of a contract” means the processing is necessary for the performance of or entering into contracts with data subjects. To determine whether the processing is “necessary for the performance of a contract”, the core requirement lies in the assessment of “necessity”. EDPB, on the basis of version for public consultation, officially issued Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version 2.0 (hereinafter referred to as the “Guidelines”) on October 8, 2019.

4.1 Assessment of Necessity

The assessment of necessity is the fundamental prerequisite for determining whether performance of contract can serve as legal basis for certain data processing activity. When assessing necessity, it shall be noted that concept of what is ‘necessary for the performance of a contract’ is not simply an assessment of what is permitted by or written into the terms of a contract.

Assessing what is ‘necessary’ involves a combined, fact-based assessment. Consideration include rights of personal data subjects, basic principles for data protection, and possible impact on the fundamental rights and freedom of the data subjects. If there are realistic, less intrusive alternatives, the processing is not ‘necessary’.

4.2 Necessary for the Performance of a Contract

A controller needs to identify the appropriate legal basis for the envisaged processing operations before the processing commences. The following prerequisites shall be fulfilled before the assessment: ① accountability, that is, data controllers can prove the legality of data processing activities; ② there shall be an effective contract.

If controllers use “necessary for the performance of a contract” as legal basis, the following questions shall be fully considered:

• What is the nature of the service being provided to the data subject? What are its distinguishing characteristics?

• What is the exact rationale of the contract?

• What are the essential elements of the contract?

• What are the mutual perspectives and expectations of the parties to the contract? Would

---

an ordinary user of the service reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract to which they are a party?

In practice, a contract may content several services based on different purposes, features or rational. To comply with the principle of fairness, the assessment of necessity shall be conducted separately within the scope of each service.

Where contract is terminated in full, then as a general rule, the processing of that data will no longer be necessary for the performance of that contract and thus the controller will need to stop processing.

4.3 Necessary for Taking Steps Prior to Entering into a Contract

“Necessary for taking steps prior to entering into a contract” refers to preliminary processing of personal data may be necessary before entering into a contract in order to facilitate the actual conclusion of a contract. It shall be noted that, in any case, this provision would not cover unsolicited marketing or other processing which is carried out solely on the initiative of the data controller, or at the request of a third party.

EDPB has given some typical examples in the Guidelines. In some cases, financial institutions have a duty to identify their customers. In line with this, before entering into a contract with data subjects, a bank requests to see their identity documents. In this case, the identification is necessary for a legal obligation on behalf of the bank rather than to take steps at the data subject’s request. Therefore, the appropriate legal basis is not “necessary for taking steps prior to entering into a contract”.

4.4 Applicability in Specific Situations

Under certain specific situations, whether data controllers can take “necessary for performance of contract” as legal basis for data processing is not clear. EDPB selected several typical situations which may cause confusion easily in the Guidelines and analyzed under these circumstances, whether “necessary for the performance of a contract” can be applied as legal basis.

Processing for “service improvement”: In most cases, collection of organisational metrics relating to a service or details of user engagement, cannot be regarded as necessary for the provision of the service as the service could be delivered in the absence of processing such personal data. In view of the EDPB, user enters into a contract to avail of an existing service. While the possibility of improvements and modifications to a service may routinely be included in contractual terms, such processing usually cannot be regarded as being objectively necessary for the performance of the contract with the user.
Processing for “fraud prevention”: processing for fraud prevention purposes may involve monitoring and profiling customers. In the view of the EDPB, such processing is likely to go beyond what is objectively necessary for the performance of a contract with a data subject.

Processing for online behavioural advertising: processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services. Further to this, “necessary for the performance of a contract” cannot provide a lawful basis for online behavioural advertising simply because such advertising indirectly funds the provision of the service.

Processing for personalization of content: The EDPB acknowledges that personalisation of content may constitute an essential; element of certain online services, and therefore maybe regarded as necessary for the performance of the contract with the service user in some cases. Whether such processing can be regarded as an intrinsic aspect of an online service, will depend on the nature of the service provided, the expectations of the average data subject and whether the service can be provided without personalisation.

Conclusion

The basic rationale on the assessment of necessity provided by the Guidelines are of great importance to companies. The exceptions for obtaining consent stipulated in Information Security Technology - Personal Information Security Specifications include request of personal information subjects and necessary for the performance of the contract. Therefore, when assessing whether a certain data processing falls under such exceptional circumstances, the basic methods and rationale for assessment of necessity provided in the Guidelines may be of reference.

5. What is Data Protection by Design and by Default

——An Interpretation on EDPB Guidelines on Article 25 Data Protection by Design and by Default

EDPB issued the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version for public consultation (hereinafter “Guidelines”) on November 13, 2019, interpreting Article 25 of the GDPR and explaining how to implement Data Protection by Design and by Default. In china, Information security technology - Personal Information Security Specification also contains similar provisions regarding personal information security engineering. Considering the relevant requirements for data protection from the beginning of product and the developing of service, and implementing design and default privacy protection throughout the lifecycle of data processing are becoming the focus of the next stage of companies’ in-depth compliance. In the following, we will focus on the contents of Guidelines and analyze the relevant industry practice and regulations in China, to put
forward corresponding suggestions on how to implement data protection by design and by default, and to improve data protection compliance capabilities.

### 5.1 Basic Concepts

Data Protection by Design and by Default (hereinafter “DPbDD”), stipulated in Article 25 of GDPR, origins from the concept of Privacy By Design, which was purposed by Dr. Ann Cavoukian in the 1970s, and was later incorporated in RL 95/46/EC Data Protection Directive.\(^{(18)}\) While Privacy By Design is a recommended good practice in the Directive, GDPR treats DPbDD as a legal requirements. Though Privacy by Design is not the same as Data Protection by Design, the relatively mature principle and practice are still applicable in the context of personal data protection.\(^{(19)}\)

(1) Data Protection by Design

*Article 25(1) of GDPR stipulates: Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

Based on this, Data Protection by Design refers to the full consideration of data protection issues in the design phase and full lifecycle of any system, service, product or process. Essentially, it is to integrate data protection into data processing activities and business practices.

(2) Data Protection by Default

*Article 25(2) of GDPR stipulates: The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their*
storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.

Based on this, Data Protection by Default refers to that only the personal data required for the purpose is processed by default, which is closely related to the principle of purpose limitation and the principle of data minimisation. Data Protection by Default requires to determine the scope of data to be processed before processing begins, and the data subject is adequately informed and the data processing is limited to the scope in relation to the purpose.

(3) The Foundational Principles of Protection by Design

Protection by Design is not at the expense of economic benefits of the product, and the following fundamental principles should be followed:

| Proactive not Reactive; Preventative not Remedial. | Privacy by Design is to proactively prevent issues before they occur, rather than seek reactively afterthought remedy. |
| Privacy as the Default Setting | Ensure that personal data is automatically protected in any given IT system or business practice. |
| Privacy Embedded into Design | Privacy by Design is embedded in the design and structure of IT systems and business practices. |
| Full Functionality: Positive-Sum, not Zero-Sum | Privacy by Design aims to satisfy all legitimate interests and purposes, rather than through a zero-sum method to balance interests and discard certain functions. |
| End-to-End Security: Full Lifecycle Protection | Before data collection, Privacy by Design should be embedded in the system and extend to the full lifecycle of the personal data involved to ensure privacy. |
| Visibility and Transparency: Keep it Open | Privacy by Design ensure that the operation of all relevant parties can be independently certificated, and is visible and transparent to users and product providers. |
| Respect for User Privacy: Keep it User-Centric | The purpose of Privacy by Design is to protect the basic rights and freedoms of individuals, and the measures taken should focus on respecting their privacy. |

5.2 The Main Contents of Guidelines

Guidelines issued by EDPB further clarifies Article 25 of GDPR and practical requirements, mainly including the application scope, analysis of the article, implementing data protection principles by using DPbDD, certification, enforcement and recommendations. These contents can be divided into two parts: What question does the Guidelines answer? What measures does the Guidelines recommend?
(1) What question does the Guidelines answer?

1) What effects will the fulfillment of DPbDD obligation bring?

According to Article 25 of GDPR and Recital 78, Guidelines clarifies there are two main purposes for fulfilling DPbDD measures: to implement the data protection principles and protect data subjects’ rights and freedom. Guidelines states that laws and regulations do not stipulate specific technical and organisational measures, as the controllers can implement measures to achieve the above purposes and demonstrate their effectiveness.

2) Who need to fulfill the obligation of DPbDD?

According to Article 25 of GDPR, the obligation of DPbDD applies to the controllers because of its right to decide the purpose and method of data processing. EDPB, as Guidelines shows, believes that data processors and technology providers shall also fulfill compliance obligations as the controllers do.

3) When to fulfill the obligation of DPbDD?

In terms of time, whether when deciding the purpose and method of processing at the beginning of the data processing activity, or in the entire process of the activities, the obligation of DPbDD shall be fulfilled to achieve continuous compliance.

4) What factors shall be considered to fulfill the obligation of DPbDD?

Guidelines explains the factors that controllers must consider when designing the process: (1) “state of the art”: controllers are required to stay up to date on technological progress in order to secure continued effective implementation of the data protection principles; (2) “cost of implementation”: this includes finance, time, labor and other costs. Guidelines highlight the high cost cannot be the reason for non-compliance; (3) “the data processing activity itself”: this includes the nature, purpose, scope, context of the processing; (4) the risk of varying likelihood and severity for rights and freedoms of natural persons posed by the processing. GDPR aims to control risks and the appropriate technical and organisational measures should be implemented.

5) How can companies benefit from fulfilling the obligation of DPbDD?

According to Guidelines, companies as the data controllers, by considering the requirements of DPbDD at the beginning phase of planning and determining data processing methods, can better implement the basic principles and compliance of GDPR; controllers can perform DPbDD certification for the data processing activities involved and use it as a market competitive advantage. If the company is a data processor or technology provider, can better assist the controller to fulfill its compliance obligations; If the data controller proposes DPbDD requirements, it can be fully realized and serve as competitive advantage.
6) How to obtain the relevant certification?

According to Article 25(3) of GDPR and Guidelines, the controller can obtain DPbDD certification under Article 42 of GDPR, which can serve as the corresponding proof of compliance. Based on Article 42 of GDPR and Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation issued on June 4, 2019, the certification can be carried out by the data protection authorities in member states of by third party. The certification body and standards shall be decided according to the actual situation of the country or region where the data processing activities occur.

(2) What measures are recommended in Guidelines?

Guidelines focuses on how to fully comply with basic principles of data protection through DPbDD, and list key elements of DPbDD for each principle, which are of great significance for companies to choose appropriate technical and organisational measures.

1) The Principle of Transparency

<table>
<thead>
<tr>
<th>Key Elements</th>
<th>Specific Requirements</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarity</td>
<td>Information shall be in clear and plain language, concise and intelligible.</td>
<td>A controller is designing a privacy policy in order to comply with the requirements of transparency. The privacy policy cannot contain a lengthy bulk of information that is difficult for the average data subject to penetrate and understand, it must be written in clear and concise language and make it easy for the user of the website to understand how their personal data is processed. The controller therefore provides information in a multi-layered manner, where the most important points are highlighted. Drop-down menus and links to other pages are provided to further explain the concepts in the policy. The controller also makes sure that the information is provided in a multi-channel manner, providing video clips to explain the most important points of the information.</td>
</tr>
<tr>
<td>Semantics</td>
<td>Communication shall have a clear meaning to the audience in question.</td>
<td></td>
</tr>
<tr>
<td>Accessibility</td>
<td>Information shall be easily accessible for the data subject.</td>
<td></td>
</tr>
<tr>
<td>Contextual</td>
<td>Information shall be provided at the relevant time and in the appropriate form.</td>
<td></td>
</tr>
<tr>
<td>Relevance</td>
<td>Information shall be relevant and applicable to the specific data subject.</td>
<td></td>
</tr>
<tr>
<td>Universal design</td>
<td>Information shall be accessible to all, include use of machine-readable languages to facilitate and automate readability and clarity.</td>
<td></td>
</tr>
<tr>
<td>Comprehensible</td>
<td>Data subjects shall have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups.</td>
<td></td>
</tr>
<tr>
<td>Multi-channel</td>
<td>Information should be provided in different channels and media, beyond the textual, to increase the probability for the information to effectively reach the data subject.</td>
<td></td>
</tr>
</tbody>
</table>
2) The Principle of Lawfulness

<table>
<thead>
<tr>
<th>Key Elements</th>
<th>Specific Requirements</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevance</td>
<td>The correct legal basis shall be applied to the processing.</td>
<td>A bank plans to offer a service to improve efficiency in the management of loan applications. The idea behind the service is that the bank, by requesting permission from the customer, can be able to retrieve data from public authorities about the customer. This may be, for example, tax data from the tax administration.</td>
</tr>
<tr>
<td>Differentiation</td>
<td>The controller shall differentiate between the legal basis used for each processing activity.</td>
<td>When implementing the principle of lawfulness, the controller realizes that they cannot use the “necessary for contract-” basis for the part of the processing that involves gathering personal data directly from the tax authorities. The fact that this specific processing presents a risk of the data subject becoming less involved in the processing of their data is also a relevant factor in assessing the lawfulness of the processing itself. The bank concludes that this part of the processing must rely on consent.</td>
</tr>
<tr>
<td>Specific purpose</td>
<td>The controller shall differentiate between the legal basis used for each processing activity</td>
<td></td>
</tr>
<tr>
<td>Necessary</td>
<td>Processing must be necessary for the purpose to be lawful. It is an objective test which involves an objective assessment of realistic alternatives of achieving the purpose.</td>
<td></td>
</tr>
<tr>
<td>Autonomy</td>
<td>The data subject should be granted the highest degree of autonomy as possible with respect to control over personal data.</td>
<td></td>
</tr>
<tr>
<td>Consent withdrawal</td>
<td>The processing shall facilitate withdrawal of consent. Withdrawal shall be as easy as giving consent. If not, any given consent is not valid.</td>
<td>The bank therefore presents information about the processing on the online application platform in such a manner that makes it easy for data subjects to understand what processing is mandatory and what is optional. The processing options, by default, do not allow retrieval of data directly from other sources than the data subject herself. Moreover, any given consent is processed electronically in a documentable manner, and data subjects are presented with an easy way of controlling what they have consented to and to withdraw their consent.</td>
</tr>
<tr>
<td>Balancing of interests</td>
<td>Where legitimate interests is the legal basis, the controller must carry out an objectively weighted balancing of interests.</td>
<td></td>
</tr>
<tr>
<td>Predetermination</td>
<td>The legal basis shall be established before the processing takes place.</td>
<td></td>
</tr>
<tr>
<td>Cessation</td>
<td>If the legal basis ceases to apply, the processing shall cease accordingly.</td>
<td></td>
</tr>
<tr>
<td>Adjust</td>
<td>If there is a valid change of legal basis for the processing, the actual processing must be adjusted in accordance with the new legal basis.</td>
<td></td>
</tr>
<tr>
<td>Default configuration</td>
<td>Processing must be limited to what the legal basis strictly gives grounds for.</td>
<td></td>
</tr>
<tr>
<td>Allocation of responsibility</td>
<td>Whenever joint controllership is envisaged, the parties must apportion in a clear and transparent way their respective responsibilities vis-à-vis the data subject.</td>
<td></td>
</tr>
</tbody>
</table>
3) The Principle of Fairness

<table>
<thead>
<tr>
<th>Key Elements</th>
<th>Specific Requirements</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomy</td>
<td>Data subjects shall be granted the highest degree of autonomy possible with respect to control over their personal data.</td>
<td>A controller processes personal data for the provision of a streaming service where users may choose between a regular subscription of standard quality and a premium subscription with higher quality. As part of the premium subscription, subscribers get prioritized customer service. With regard to the fairness principle, the prioritized customer service granted to premium subscribers cannot discriminate other data subjects’ rights according to the GDPR Article 12. This means that although the premium subscribers get prioritized service, such prioritization cannot result in a lack of appropriate measures to respond to request from regular subscribers without undue delay. Prioritized customers may pay to get better service, but all data subjects shall have equal and indiscriminate access to enforce their rights and freedoms according to the GDPR.</td>
</tr>
<tr>
<td>Interaction</td>
<td>Data subjects must be able to communicate and exercise their rights with the controller.</td>
<td></td>
</tr>
<tr>
<td>Expectation</td>
<td>Processing should correspond with data subjects’ expectations.</td>
<td></td>
</tr>
<tr>
<td>Non-discrimination</td>
<td>The controller shall not discriminate against data subjects.</td>
<td></td>
</tr>
<tr>
<td>Non-exploitation</td>
<td>The controller shall not exploit the needs or vulnerabilities of data subjects.</td>
<td></td>
</tr>
<tr>
<td>Consumer choice</td>
<td>The controller should not “lock in” their users. Whenever a service or a good is personalized or proprietary, it may create a lock-in to the service or good. If it is difficult for the data subject to change controllers due to this, which may not be fair.</td>
<td></td>
</tr>
<tr>
<td>Power balance</td>
<td>Asymmetric power balances shall be avoided or mitigated when possible. Controllers should not transfer the risks of the enterprise to the data subjects.</td>
<td></td>
</tr>
<tr>
<td>Respect rights and freedoms</td>
<td>The controller must respect the fundamental rights and freedoms of data subjects and implement appropriate measures and safeguards to not violate these rights and freedoms.</td>
<td></td>
</tr>
<tr>
<td>Ethical</td>
<td>The controller should see the processing’s wider impact on individuals’ rights and dignity.</td>
<td></td>
</tr>
<tr>
<td>Truthful</td>
<td>The controller must act as they declare to do, provide account for what they do and not mislead the data subjects.</td>
<td></td>
</tr>
<tr>
<td>Human intervention</td>
<td>The controller must incorporate qualified human intervention that is capable of recovering biases that machines may create in relation to the right to not be subject to automated individual decision making.</td>
<td></td>
</tr>
<tr>
<td>Fair algorithm</td>
<td>Information shall be provided to data subjects about processing of personal data based on algorithms that analyze or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behavior, location or movements.</td>
<td></td>
</tr>
</tbody>
</table>
4) The Principle of Purpose Limitation

<table>
<thead>
<tr>
<th>Key Elements</th>
<th>Specific Requirements</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predetermination</td>
<td>The legitimate purposes must be determined before the design of the processing.</td>
<td>A controller processes personal data about its customers. The purpose of the processing is to fulfill a contract, i.e. to be able to deliver goods to the correct address and obtain payment. The personal data stored is the purchase history, name, address, e-mail address and telephone number.</td>
</tr>
<tr>
<td>Specificity</td>
<td>The purposes must be specific to the processing and make it explicitly clear why personal data is being processed.</td>
<td>The controller is considering buying a Customer Relationship Management (CRM) product that gathers all the customer data such as sales, marketing and customer service in one place. The product gives the opportunity of storing all phone calls, activities, documents, emails and marketing campaigns to get a 360-degree view of the customer. Ultimately the CRM automatically analyses the customers’ purchasing power by using public information. The purpose of the analysis is to target the advertising better but is not a part of the original lawful purpose of the processing.</td>
</tr>
<tr>
<td>Purpose orientation</td>
<td>The purpose of processing should guide the design of the processing and set processing boundaries.</td>
<td>The controller must regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.</td>
</tr>
<tr>
<td>Necessity</td>
<td>The purpose determines what personal data is necessary for the processing.</td>
<td>The controller must regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.</td>
</tr>
<tr>
<td>Compatibility</td>
<td>Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design.</td>
<td>The controller requires the provider of the product to map the different processing activities using personal data with the purposes relevant for the controller. Another requirement is that the product shall be able to flag which kind of processing activities using personal data that is not in line with the legitimate purposes of the controller. After receiving the results of the mapping, the controller assesses whether the new marketing purpose and the targeted advertisement purpose are within the contractual purposes or if they need another legal ground for this processing. Alternatively, the controller could choose to not make use of this functionality in the product.</td>
</tr>
<tr>
<td>Limit further processing</td>
<td>The controller should not connect datasets or perform any further processing for new incompatible purposes.</td>
<td>To be in line with the principle of purpose limitation, the controller requires the provider of the product to map the different processing activities using personal data with the purposes relevant for the controller. Another requirement is that the product shall be able to flag which kind of processing activities using personal data that is not in line with the legitimate purposes of the controller. After receiving the results of the mapping, the controller assesses whether the new marketing purpose and the targeted advertisement purpose are within the contractual purposes or if they need another legal ground for this processing. Alternatively, the controller could choose to not make use of this functionality in the product.</td>
</tr>
<tr>
<td>Review</td>
<td>The controller must regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.</td>
<td>To be in line with the principle of purpose limitation, the controller requires the provider of the product to map the different processing activities using personal data with the purposes relevant for the controller. Another requirement is that the product shall be able to flag which kind of processing activities using personal data that is not in line with the legitimate purposes of the controller. After receiving the results of the mapping, the controller assesses whether the new marketing purpose and the targeted advertisement purpose are within the contractual purposes or if they need another legal ground for this processing. Alternatively, the controller could choose to not make use of this functionality in the product.</td>
</tr>
<tr>
<td>Technical limitations of reuse</td>
<td>The controller must regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.</td>
<td>To be in line with the principle of purpose limitation, the controller requires the provider of the product to map the different processing activities using personal data with the purposes relevant for the controller. Another requirement is that the product shall be able to flag which kind of processing activities using personal data that is not in line with the legitimate purposes of the controller. After receiving the results of the mapping, the controller assesses whether the new marketing purpose and the targeted advertisement purpose are within the contractual purposes or if they need another legal ground for this processing. Alternatively, the controller could choose to not make use of this functionality in the product.</td>
</tr>
</tbody>
</table>
5) The Principle of Data Minimisation

<table>
<thead>
<tr>
<th>Key Elements</th>
<th>Specific Requirements</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data avoidance</td>
<td>Avoid processing personal data altogether when this is possible for the relevant purpose.</td>
<td>A public transportation company wishes to gather statistical information based on travelers’ routes. This is useful for the purposes of making proper choices on changes in public transport schedules and proper routings of the trains. The passengers must pass their ticket through a reader every time they enter or exit a means of transport. Having carried out a risk assessment related to the rights and freedoms of passengers’ regarding the collection of passengers’ travel routes, the controller establishes that it is possible to identify the passengers based on the ticket identifier. Therefore, since it is not necessary for the purpose of optimizing the public transport schedules and routings of the trains, the controller does not store the ticket identifier. Once the trip is over, the controller only stores the individual travel routes so as to not be able to identify trips connected to a single ticket, but only retains information about separate travel routes. In cases where there can be a risk of identifying a person solely by their travel route (this might be the case in remote areas) the controller implements measures to aggregate the travel route.</td>
</tr>
<tr>
<td>Relevance</td>
<td>Personal data shall be relevant to the processing in question, and the controller shall be able to demonstrate this relevance.</td>
<td></td>
</tr>
<tr>
<td>Necessity</td>
<td>Each personal data element shall be necessary for the specified purposes and should only be processed if it is not possible to fulfil the purpose by other means.</td>
<td></td>
</tr>
<tr>
<td>limitation</td>
<td>Limit the amount of personal data collected to what is necessary for the purpose.</td>
<td></td>
</tr>
<tr>
<td>Aggregation</td>
<td>Use aggregated data when possible.</td>
<td></td>
</tr>
<tr>
<td>Pseudonymization</td>
<td>Pseudonymize personal data as soon as it is no longer necessary to have directly identifiable personal data, and store identification keys separately.</td>
<td></td>
</tr>
<tr>
<td>Anonymization and deletion</td>
<td>Where personal data is not, or no longer necessary for the purpose, personal data shall be anonymized or deleted.</td>
<td></td>
</tr>
<tr>
<td>Data flow</td>
<td>The data flow shall be made efficient enough to not create more copies, or entry points for data collection than necessary.</td>
<td></td>
</tr>
<tr>
<td>State of the art</td>
<td>The controller should apply available and suitable technologies for data avoidance and minimisation.</td>
<td></td>
</tr>
</tbody>
</table>
### 6) The Principle of Accuracy

<table>
<thead>
<tr>
<th>Key Elements</th>
<th>Specific Requirements</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data source</td>
<td>Data sources should be reliable in terms of data accuracy.</td>
<td>A bank wishes to use artificial intelligence (AI) to profile customers applying for bank loans as a basis for their decision making. When determining how their AI solutions should be developed, they are determining the means of processing and must consider data protection by design when choosing an AI from a vendor and when deciding on how to train the AI. When determining how to train the AI, the controller must have accurate data to achieve precise results. Therefore, the controller must ensure that the data used to train the AI is accurate. Granted they have the legal basis to train the AI using personal data from a large pool of their existing customers, the controller chooses a pool of customers that is representative of the population to also avoid bias. Meanwhile, the latest data can be selected to ensure the accuracy of personal data as much as possible. Moreover, the bank should also fully evaluate the reliability of AI and whether it provides non-discriminatory results. After maturely training AI and putting it into use, the bank should use the AI profile results as part of the loan evaluation, and should not make loan decisions based solely on it. At the same time, it should also periodically review the accuracy of the AI results.</td>
</tr>
<tr>
<td>Degree of accuracy</td>
<td>Each personal data element shall be as accurate as necessary for the specified purposes.</td>
<td></td>
</tr>
<tr>
<td>Measurably accurate</td>
<td>Reduce the number of false positives/negatives.</td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td>Depending on the nature of the data, in relation to how often it may change, the controller should verify the correctness of personal data with the data subject before and at different stages of the processing.</td>
<td></td>
</tr>
<tr>
<td>Erasure/rectification</td>
<td>The controller must erase or rectify inaccurate data without delay.</td>
<td></td>
</tr>
<tr>
<td>Accumulated errors</td>
<td>Controllers must mitigate the effect of an accumulated error in the processing chain.</td>
<td></td>
</tr>
<tr>
<td>Access</td>
<td>Data subjects should be given an overview and easy access to personal data in order to control accuracy and rectify as needed.</td>
<td></td>
</tr>
<tr>
<td>Continued accuracy</td>
<td>Personal data should be accurate at all stages of the processing, tests of accuracy should be carried out at critical steps.</td>
<td></td>
</tr>
<tr>
<td>Up to date</td>
<td>Personal data shall be updated if necessary for the purpose.</td>
<td></td>
</tr>
<tr>
<td>Data design</td>
<td>Use of technological and organisational design features to decrease inaccuracy, • e.g. drops down lists with limited values, internal policies, and legal criteria.</td>
<td></td>
</tr>
</tbody>
</table>
7) The Principle of Storage Limitation

<table>
<thead>
<tr>
<th>Key Elements</th>
<th>Specific Requirements</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletion</td>
<td>The controller must have clear internal procedures for deletion.</td>
<td>A bank should also fully evaluate the reliability of AI and whether it provides non-discriminatory results. After maturely training AI and putting it into use, the bank should use the AI profile results as part of the loan evaluation, and should not make loan decisions based solely on it. At the same time, it should also periodically review the accuracy of the AI results.</td>
</tr>
<tr>
<td>Automation</td>
<td>Deletion of certain personal data should be automated.</td>
<td>To make deletion more effective, the controller instead implements an automatic system to delete data automatically and more regularly. The system is configured to follow the given procedure for data deletion which then occurs at a predefined regular interval to remove personal data from all of the company's storage media</td>
</tr>
<tr>
<td>Storage criteria</td>
<td>The controller must determine what data and length of storage is necessary for the purpose.</td>
<td></td>
</tr>
<tr>
<td>Enforcement of retention</td>
<td>The controller must enforce internal retention policies and conduct tests of whether the organization practices its policies.</td>
<td></td>
</tr>
<tr>
<td>policies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8) The Principle of Integrity and Confidentiality

<table>
<thead>
<tr>
<th>Key Elements</th>
<th>Specific Requirements</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISMS</td>
<td>Have an operative means of managing policies and procedures for information security. For some controllers, this may be possible with the help of an ISMS.</td>
<td>A controller wants to extract personal data from a medical database to a server in the company. The company has assessed the risk for routing the extracts to a server that is accessible to all of the company's employees as likely to be high for data subjects' rights and freedoms. There is only one department in the company who needs to process these patient data.</td>
</tr>
<tr>
<td>Risk analysis</td>
<td>Assess the risks against the security of personal data and counter identified risks.</td>
<td>To regulate access and mitigate possible damage from malware, the company decides to segregate the network, and establish access controls to the server and the directory. In addition, they put up security monitoring and an intrusion detection and prevention system. The controller activates access control on the server and isolates it from routine use. An automated auditing system is put in place to monitor access and changes.</td>
</tr>
<tr>
<td>Resilience</td>
<td>The processing should be robust enough to withstand changes, regulatory demands, incidents and cyber attacks</td>
<td></td>
</tr>
<tr>
<td>Access management</td>
<td>Only authorized personnel shall have access to the data necessary for their processing tasks.</td>
<td></td>
</tr>
<tr>
<td>Secure transfer</td>
<td>Transfers shall be secured against unauthorized access and changes.</td>
<td></td>
</tr>
<tr>
<td>Secure storage</td>
<td>Data storage shall be secure from unauthorized access and changes.</td>
<td></td>
</tr>
<tr>
<td>Backup/logs</td>
<td>Keep back-ups and logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control.</td>
<td></td>
</tr>
<tr>
<td>Special protection</td>
<td>Special categories of personal data should be protected with adequate measures and, when possible, be kept separated from the rest of the personal data.</td>
<td></td>
</tr>
<tr>
<td>Key Elements</td>
<td>Specific Requirements</td>
<td>Example</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Pseudonymization</td>
<td>Personal data and back-ups/logs should be pseudonymized as a security measure to minimize risks of potential data breaches, for example using hashing or encryption.</td>
<td>Reporting and automated alerts are generated from this when certain events related to usage are configured. This security measure will ensure that all users have access on a need to know basis and with the appropriate access level. Inappropriate use can be quickly and easily recognized. The preventative and effective measures and safeguards should be built into all personal data processing undertakes now and in the future doing so may help prevent future such data breach incidents.</td>
</tr>
<tr>
<td>Security incident response management</td>
<td>Have in place routines and procedures to detect, handle, report and learn from data breaches</td>
<td></td>
</tr>
<tr>
<td>Personal data breach handling</td>
<td>Integrate management of notification (to the supervisory authority) and information (to data subjects) obligations in the event of a data breach into security incident management procedures.</td>
<td></td>
</tr>
<tr>
<td>Maintenance and development</td>
<td>Regular review and test software to uncover vulnerabilities of the systems supporting the processing.</td>
<td></td>
</tr>
</tbody>
</table>

### 5.3 Lessons for Compliance

DPbDD is of great significance for personal data protection compliance and has always been one of the key topics in making personal data protection regulations. Besides the Guidelines, the Spanish data protection authority AEPD (Agencia Española de Protección de Datos) issued A Guide to Privacy by Design shortly before EDPB published Guidelines. Moreover, ISO 27701 (ISO/IEC 27701 Privacy Information Management), the latest achievement in international privacy management, also stipulates DPbDD as one of the obligations for controllers and processors.

Similarly, Information Security Technology—Guidelines for Personal Information Security Engineering, issued by National Information Security Standardization Technical Committee (SAC/TC260) on May 28, 2019 also shows the idea of DPbDD by setting personal data protection requirements on phases in the stages of demand analysis, product design, product development, test review and release, to ensure products can meet the relevant demands of personal data protection.

To achieve compliance from the design phase, DPbDD emphasizes that the product itself is compliant, which is the general trend of personal data protection compliance work. Companies can refer to Guidelines and related regulations, specifications and fully consider and implement compliance obligations at the beginning of product design, balance the business development and privacy protection, provide customers with products of compliance, establishing user trust, enhance market competition ability.
6. The Application of GDPR in the Scenario of Video Devices

—An Interpretation of EDPB Guidelines on processing personal data through video devices

Preamble

Video devices can be found everywhere in today’s daily life. Surveillance cameras in the streets, shopping malls and communities, and facial recognition devices such as mobile payment are collecting and processing our personal data all the time. With the continuous development of facial recognition technology, video devices are widely used in fields like public security, new retail, mobile payment, etc. The personal data protection issues have aroused concern of the whole society.

In the personal data protection framework of GDPR, the personal data processing activities of personal data controllers through video devices are personal data processing activities in the particular situation. Besides meeting the requirements of GDPR, full attention shall also be paid to the issues that require special attention in this particular situation.

EEDPB released Guidelines 3/2019 on processing personal data through video devices -version for public consultation on July 10, 2019, and officially issued Guidelines 3/2019 on processing personal data through video devices-version 2.0\(^{20}\) (hereinafter referred to as the “Guidelines”) on January 20, 2020, which provides ample references for companies to collect and process personal data through video devices in accordance with the compliance requirements of GDPR in practice.\(^{21}\)

We will interpret the Guidelines from five aspects: the lawfulness of personal data processing activities, data minimisation, protection of personal data subject rights, disclosure management to third parties and other risk control measures.

6.1 Lawfulness of Personal Data Processing Activities

(1) For General Categories of Personal Data

Video Devices can serve many purposes, e.g. for the protection of life, security of property and other assets, collecting evidence. According Article 5 and Article 6 of GDPR, personal data controllers should refine and clarify the processing purpose in accordance with the specific scenario, and judge the legal basis on which the personal data processing activities are based. In the scenario of processing personal data through video devices, the most


\(^{21}\) It should be noted that personal data processing activities carried out by a natural person in the course of a purely personal or household activities are not governed for GDPR. Therefore, the personal data processing activities performed by a natural person through video devices in the above situations are not covered by the relevant requirements of the guidelines. However, once a natural person chooses to publish personal data on the Internet (for example, a blogger posts a lifestyle vlog on a video website), it will exceed the scope of the above exemption and need to comply with GDPR and the Guidelines.
commonly used legal basis for personal data controllers is legitimate interests and the
consent given by the data subject. In some special scenarios, necessity to perform a task
carried out in the public interest or in the exercise of official authority under Article 6(1)(e)
of GDPR can also be a proper legal basis.

A. Legitimate Interests

If the personal data controller applies the legitimate interest as the legal basis on which the
data processing activities are based, it should conduct a strict proof. The Guidelines combine
with the basic steps of judging legal basis of personal data processing activities in the Guide
to GDPR issued by the Information Commission’s Office (ICO) of the U.K.22, providing detailed
guidance on the circumstances under which personal data controllers can conduct personal
data processing activities through video devices based on legitimate interests.

The first step: the identification of legitimate interests. The legitimate interests of the
personal data controller should be of real existence that are sufficiently clear and necessary,
such as the legitimate interests of protecting property security through video surveillance in
practice.

The second step: the necessity test. Data processing activities should be necessary for
personal data controllers to achieve a specific purpose. Generally speaking, in the scenario
of personal data processing activities through video devices, since the video devices may
involve the shooting of all personal data subjects passing by, for the purpose of protecting
the property, the monitoring scope of the video devices should be limited to the reasonable
boundaries of the property itself. For example, if a store installs a camera for security
purposes, the monitored range should be limited to the door of the store and cannot be
expanded to the driveway of the door.

The third step: the balancing test. The legitimate interests of personal data controllers
cannot override the fundamental rights and freedoms of personal data subjects. If behaviors
such as video surveillance involve serious violations of the privacy of the data subjects, the
personal data controller can no longer use legitimate interests as the legal basis.

B. Consent of the Personal Data Subject

GDPR has a relatively strict requirements for personal data subject consent. Only when the
personal data subject needs to voluntarily make a specific, informed, unambiguous, and
withdraw-able intention, and the personal data controller can provide the corresponding
proof of the above consent, the consent of the personal data subject is valid. Considering
the wide range and uncertainty in the scenario of processing personal data through video

devices, the Guidelines purposes that the consent of the personal data subject can be used as the legal basis only in rare cases.

(2) For Special Categories of Personal Data

The special categories of personal data in GDPR refer to the information related to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. The general opinion will mistakenly believe that video devices involve the collection of biometric data due to directly capturing human faces. In fact, personal data collected through video devices does not necessarily constitute biometric data, it only constitutes a special category of individuals under the GDPR when it is used to identify specific individuals or to infer personal characteristics related to special categories of personal data.

In principle, GDPR prohibits the processing of special categories of personal data. Personal data controllers may only collect and process special categories of personal data under limited exceptions, such as obtaining the personal data subject’s express consent, the personal data subject’s disclosure of the corresponding special category of personal data, or the protection of the significant interests of others. Therefore, if the personal data controller uses video devices for some special purposes to constitute the processing of special categories of personal data, the personal data controller should determine the applicable exceptions based on the specific scenario and the processing purpose, while fully considering data processing methods and other factors to avoid illegal processing of special categories of personal data.

6.2 Data Minimisation

According to Article 5 of GDPR, personal data controller should process personal data limited to the necessary scope in relation to the purposes. To realize data minimisation, when personal data controllers collect and process personal data through video devices, they should ensure that the collection, storage and use of the various phases are limited to a certain scope.

In the collection phase, the personal data controller can avoid excessive collection of personal data by adjusting the shooting range, angle, time, etc. of the video devices. In the storage phase, the personal data controller should ensure that the video devices only store the necessary period for the specific processing purpose. For instance, when the video surveillance is set for the purpose of property protection or preservation of evidence, the relevant people could make decisions within one or two days, and in ideal situations, video devices can be set automatically erase personal data after a certain number of days. If the personal data controllers need to store personal data for a longer period of time, it should
fully demonstrate its legality and necessity. In the phase of use, personal data controllers should limit the internal permission and disclosure of personal data, and avoid using personal data for other purposes.

6.3 Protection of Data Subject Rights

(1) Protection of Data Subjects’ Right to be Aware

The protection of data subjects’ right to be aware is an embodiment of the principle of transparency under GDPR. When the personal data controller processes personal data through the video device, he should ensure that the personal data subject is fully informed about the fact that the video device is processing its personal data.

In light of the characters of video devices, the Guidelines suggest the personal data controller should fully inform data subjects following a two-layer approach.

For the first layer, personal data controller should show the most important information by posting or placing a warning sign in obvious places that can be easily noticed by personal data subjects. The Warning sign should generally convey the content including purposes of processing, the identity of the controller, legitimate interests (if applicable), reference for personal data subject to read detailed contents and other information.

For the second layer, personal data controller should use other appropriate means to inform personal data subjects regarding detailed information of processing his personal data and can send message or take technical measures (e.g. QR-code referring to detailed contents for personal data subjects to read) to inform personal data subject the identity of the controller, contact information, purpose of processing, categories of personal data, the legal basis, storage position and period, rights of data subjects and other complete information.

(2) Protection of Other Personal Data Rights

The Guidelines focuses on the implementation and protection of the right to access, the right to erase and the right to object in the scenario of processing personal data through video devices.

For personal data subjects’ right to access, in cases that complying with a data subject’s request for rights may affect the rights of other data subject, or objectively unable to identify specific information from plentiful screenings for the data subject to access, the personal data controller should fully explain to the personal data subject why the right request cannot be fulfilled within the time limit promised.

For personal data subjects’ right to erasure, if the personal data controller discloses
corresponding video information through online publishing or other approaches, once the personal data subject reasonably requests to erase his personal data, the personal data controller should notify relevant third party in time while erasing the data.

For personal data subjects’ right to object, the Guidelines clarify that personal data subjects in the following to situations have the right to object, and accordingly, the personal data controller shall stop the processing activities in time: the first is that personal data controllers use legitimate interests as the legal basis to process their personal data through video devices; the second is that the personal data controller use the necessity for the performance of a task carried out in the public interest or in the exercise of official authority. If the personal data subject objects to the processing of his personal data.

6.4 Disclosure Management to Third Parties

When the personal data controller processes personal data through video devices, if it is necessary to disclose the corresponding personal data to a third party, it should ensure that the disclosure does not exceed the purpose for the personal data collection. At the same time, as a kind of personal data processing activity, this disclosure should have a corresponding legal basis. For instance, in the case to disclose personal data processed by video devices to law enforcement agencies to assist the law enforcement, the personal data can use the necessity for compliance a legal obligation under Article 6(1)(c) of GDPR as the legal basis to disclose to the law enforcement agencies. Moreover, if the disclosure process involves cross-border transmission of personal data, the personal data controller should also obey the related requirements of personal data cross-border transmission.

6.5 Other Risk Control Measures

In addition to the analysis and suggestions for the above basic issues, the guidelines proposes that personal data controllers can adopt Data Protection by Design and by Default (“DPbDD”) and Data Protection Impact Assessment (“DPIA”) as effective risk control measures.

(1) DPbDD

DPbDD refers to the requirement that the personal data controller fully integrates the protection of personal data at the beginning of the product or service design, to ensure that only the minimum necessary personal data is processed by default. In order to fulfill the requirements of DPbDD, personal data controllers should take technical measures such as encryption, anonymization, access control, and appropriate organizational measures, for example, after fully considering the purpose of using video devices, the scope of coverage, personnel management and other factors, making policies or procedures for the processing personal data through video devices, to achieve the legal processing and safeguard of personal data.
(2) DPIA

DPIA refers to the requirement that personal data controller should carry out assessment of the risk of personal data processing activities in specific scenarios and make suggestions in response of the risk. According to Article 35 of GDPR, if personal data processing activities are likely to result in a high risk to the rights and freedoms of personal data subjects, DPIA should be conducted. Among them, the monitoring of a publicly accessible area on a large scale is a typical scenario. Due to the uncertainty of the number and scope of personal data subjects covered by video device monitoring, the Guidelines recommends that before using video devices for surveillance and other purposes, personal data controller should conduct DPIA for this specific scenario.

Conclusion

Nowadays, processing personal data through video devices is a common personal data processing activity. Personal data controllers should fully comply with the basic requirements of various personal data processing activities, while paying full attention to the special requirements in this scenario. In our country, when companies use video devices to collect and process personal data, they can refer to the relevant analysis and risk control measures in the Guidelines to protect the rights of personal data subjects more effectively.

7. Personal Data Risks and Countermeasures in the Context of IoV under GDPR

——An Interpretation on EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications

Preamble

With the continuous development of connected vehicle technology, connected vehicles have gradually entered the mainstream market, and traditional car manufacturers have undergone digital transformation, building a connected vehicle ecosystem with many traditional automotive industry and emerging digital economy industry participants. Due to the complexity of the connected vehicle ecosystem and the closeness of the interconnection of the personal data processing activities of all participants in this process, the combined personal data protection issues have aroused wide concern of the whole society.

In the personal data protection framework of GDPR, EDPB released Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications - version for public consultation (hereinafter referred to as the “Guidelines”) on January 28, 2020, which clearly explains the privacy and data protection risks in personal data protection of connected vehicles. In this chapter, the Guidelines will be introduced in detail and the application of the Guidelines in the context of IoV under GDPR will be explained in detail.

data processing activities under the context of connected vehicles and corresponding countermeasures, with great reference significance for all parties in the connected vehicle industry.

7.1 Personal Data in the Context of Connected Vehicles.

In various complex contexts of connected vehicles like mobility management, vehicle management, road safety, entertainment, drive assistance, well-being, no matter whether the car itself is connected to the Internet or not, personal data can be collected through several means including vehicle sensors, Vehicle T-BOX\(^{24}\) (telematics box or mobile applications (e.g. accessed from a device belonging to a driver).

In the traditional sense, vehicle-related data may not constitute personal data, but in the connected vehicle context, much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitutes personal data under GDPR. It includes the identifiable data (e.g., the driver’s complete identity) as well as indirectly identifiable data, like vehicle usage data (e.g., data relating to driving distance covered) and vehicle’s technical data (e.g., data relating to the wear and tear on vehicle parts). Such data and other information, especially the vehicle identification number (VIN) can be associated to identify a natural person.

Specifically, the scope of the Guidelines focuses on the personal data of data subjects: e.g., vehicle owners, drivers, passengers, renters, etc. It deals with the personal data (i) processed inside the vehicle, (ii) exchanged between the vehicle and personal devices connected to it (e.g., the car owners’, drivers’ or passengers’ smartphones) and (iii) collected within the vehicle and exported to external entities (e.g., vehicle manufactures, infrastructure managers, insurance companies, car repairers) for further processing.

Meanwhile, the Guidelines also clarifies that personal data based on the employment relationship in the connected vehicle context, personal data related to built-in WiFi in cars, and personal data related to Cooperative Intelligent Transport Systems (C-ITS), due to their particularity, are out of the scope of the Guidelines.

7.2 Personal data Processing Risks in the Context of Connected Vehicles

Parties involved in personal data processing activity in the context of connected vehicles may include vehicle manufactures, equipment manufacturers, car repairers, automobile dealerships, vehicle service providers, rental and car sharing companies, fleet managers, motor insurance companies, entertainment providers, telecommunication operators, road infrastructure managers and public authorities, etc. Due to the different and roles of the

---

24 Vehicle T-BOX, also known as vehicle communication terminal, is mainly used to communicate with background system/mobile phone APP, to realize vehicle information display and control by mobile phone APP.
participating parties in the connected vehicles ecosystem, the corresponding personal data protection risks faced by various parties are different. The Guidelines summarize the following typical risks of personal data processing activities in the context of connected vehicles:

(1) Lack of Control and Information Asymmetry

For one thing, information related to personal data processing activities might only be acknowledged by the vehicle owners (e.g. providing the vehicle owners with the relevant content specified in the privacy policy or car purchase agreement when buying cars), not by the drivers or passengers. This can lead to the absence of effectively control over personal data for the personal data subjects that are actually affected.

For another, considering the complexity of connected vehicle technology, personal data subject cannot fully understand the specific situations of the processing of their personal data. This can trigger collecting and processing activities of personal data automatically by default, without the individual being aware of it.

(2) Non-Validity of Personal Data Subjects’ Consent

According to European Commission’s ePrivacy Directive, storing information or gaining access to information stored in the terminal equipment is allowed on the condition of obtaining personal data subjects’ content. This provision shall prevail over the application of Article 6 of GDPR regarding legal basis. In the context of connected vehicles, the connected vehicle any device connected to it will constitute a terminal device, so the storage and access to data in such devices should obtain consent of the personal data subject in advance.

According to the Guidelines on consent under Regulation 2016/679 issued by WP29 after the release of the Guidelines on processing personal data in the context of connected vehicles and mobility related applications, a valid consent shall be freely given, specific, informed, unambiguous indication of the data subject’s wishes, withdrawable and the data subject can demonstrate. In the context of connected vehicles, the personal data subject may not be aware of the data processing carried out in the vehicle, and cannot make valid consent on the basis of being informed; Besides, consent might also be difficult to obtain for drivers and

25 Directive 2002/58/EC of the European Parliament and of the Council Directive on privacy and electronic communications (ePrivacy Directive) Article 5(3): Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

26 Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019.


passengers who are not related to the vehicle’s owner in the case of second-hand, leased, rented or borrowed vehicles.

(3) Lack of Legal Basis for Further Processing of Personal Data

As for personal data processing activities, the participating parties shall strictly follow the principles of purpose limitation and data minimisation, to collect personal data within the scope in relation to the purpose. If the parties see for further personal data processing, and the new processing activity is not compatible with the original purpose, there shall be new legal basis. For example, telemetry data, which is collected during the use of the vehicle for maintenance purposes may not be disclosed to motor insurance companies without the driver's consent to offer driving behavior-based insurance policies.

As for assisting law enforcement authorities, if the specific conditions are fulfilled, the law enforcement authorities may collect data to detect speeding or other infractions. It should be noted that as EDPB points out, the processing of personal data for the sole purpose of fulfilling the requests made by law enforcement authorities does not constitute a specified, explicit and legitimate purpose within the meaning of Art 5 of GDPR. Only when the law enforcement authorities are authorized by the law to be third parties under GDPR, can the manufacturers provide them with data of personal data subjects in compliance with the relevant legal framework in each Member State.

(4) Excessive Data Collection

In the context of connected vehicles, due to the complexity and cutting-edge nature of connected vehicle technology, for one thing the number of sensors is ever-increasing, making the scale of data collection larger and the categories of data more various, resulting in the risks of excessive data collection; for another, the development of new functionalities of connected vehicles is based on machine learning algorithms, which may require a large amount of data collected over a long period of time, also giving rise to the risk of excessive data collection.

(5) High Risk of Personal Data Security

Due to the critical level of the connected vehicles system itself and the high participation of natural persons in the context, the security breach may endanger the life and health of individuals, cause damage to the significant interests of natural persons.

The security risks faced by connected vehicles mainly come from two aspects: first, the plurality of functionalities, services and interfaces increase possibility of the cybersecurity attack; second, personal data stored on vehicles and/or at external locations (e.g., in clouding computing infrastructures) may not be adequately secured.
7.3 Risk Countermeasures for Personal Data Processing in the Context of Connected Vehicles

To mitigate the risk for data subjects in the context of connected vehicles, and avoid damage to data subjects’ fundamental rights, freedom, and public interests, the Guidelines propose basic recommendations for the typical risks mentioned above, providing adequate references for parties involving in personal data processing activities.

(1) Three Categories of Personal Data to be Focused on

Most data associated with connected vehicles will be considered personal data to the extent that it is possible to link it to one or more identifiable individuals. EDPB has identified three categories of personal data warranting special attention: geolocation data, biometric data and data revealing criminal offenses or other infractions.

Collecting geolocation data is subject to compliance with the following principles:

(i) adequate configuration of the frequency of access to, and of the level of detail of, geolocation data collected relative to the purpose of processing. For example, a weather application should not be able to access the vehicle’s geolocation every second, even with the consent of the data subject;

(ii) providing accurate information on the purpose of processing;

(iii) when the processing is based on consent, obtaining valid consent that is distinct from the general conditions of sale or use, for example on the onboard computer;

(iv) activating geolocation only when the user launches a functionality that requires the vehicle location to be known, and not by default and continuously when the car is started;

(v) informing the user that geolocation has been activated, in particular by using icons;

As for the collection and usage of biometric data, firstly, the involving parties shall provide personal data subject with non-biometric alternative, and not impose additional constraints on personal data subjects; secondly, after collecting biometric data, the parties shall ensure the security of the data in following aspects: (i) storing and comparing the biometric template in encrypted form only on a local basis, with biometric data not being processed by an external reading/comparison terminal; (ii) ensuring the biometric authentication solution is sufficiently reliable for security protection; (iii) avoiding storing raw data, which constitutes processing of data for biometric template and user authentication in real time.

For collection and usage of data revealing criminal offenses or other infractions, EDPB
recommends to resort to the local processing of the data, to ensure the data subjects have full control over the processing, and protect against illegitimate access, modification and deletion of those data. Except for some exceptions, external processing of data revealing criminal offenses or other infractions is forbidden.

(2) Principles of Purpose limitation and Data Minimisation

According to GDPR, the purpose for processing personal data should be specified, explicit and legitimate, and every processing activity should have corresponding legal basis. The personal data processing activities should be limited to the extent necessary for the purpose. To comply with the data minimisation principle, in collecting personal data, the involved party should pay special attention to the categories of data, and only collecting data that are relevant and necessary in the minimum scope; in using personal data, participants should ensure the use falls within the scope of the purpose clarified when collecting data, and the processing as well as storing of personal data should be limited to what is necessary in relation to the purpose.

(3) Data Protection by Design and by Default

Data Protection by Design and by Default (DPbDD) refers to full consideration of data protection issues in the design phase and the whole lifecycle of any system, service product or phase, while ensuring that only the personal data necessary for the purpose is processed by default. The Guidelines propose general practice that can be referenced for all participants in the context of connected vehicles, and they should try to do as:

(i) Process personal data locally to ensure personal data subjects have control over their own personal data. It is also recommended to develop secure in-car application platform, physically divided from safety relevant car functions so that the access to car data does not depend on un necessarily external cloud capabilities;

(ii) If data must leave the vehicle, anonymize it before being transmitted.

(iii) Given the scale and sensitivity of the personal data that can be generated via connected vehicles, it is likely that processing-particularly in situations where personal data are processed outside of the vehicle-will often result in a high risk to the rights and freedoms of individuals. The Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version for public consultation issued by EDPB on November 13, 2019 provides a

---

29 According to Article 35 of GDPR and Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 issued by WP29 in 2017, when data processing activities are likely to result in a high risk for the fundamental rights and freedom of the natural person, DPIA shall be conducted before processing personal data. The typical situations in which DPIA shall be conducted include: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.
comprehensive introduction to the specific measures to achieve DPbDD. Please read Jades from Other Mountain: EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default we published before to learn more.

(4) Protection the Rights of Personal Data Subjects

To protect the rights of personal data subjects, prior to the processing of personal data, the data subject shall be informed of the identity of the data controller, the purpose of processing, the data recipients, the period for which data will be stored, and the data subject’s rights, etc. In cases personal data is not collected directly from individuals (e.g. a vehicle and equipment manufacturer may rely on a dealer to collect information about the owner of the vehicle in order to offer an emergency road side assistance service), the above mentioned information can be informed to data subjects by clauses in documents like the contract of sale of the vehicle, in the contract for the provision of services or the on-board screen.

Additionally, participants should facilitate data subjects’ control over their data during the entire processing period, through the implementation of specific tools providing an effective way to exercise their rights. To help data subjects easily change their privacy settings, a profile management system should be implemented inside the vehicle by manufacturers.

(5) Strengthening Data Security Protection

To control the security risk of data in the context of connected vehicles, participants should take all effective measures that guarantee the security and confidentiality of processed data, like encrypting the communication channels, putting in place an encryption-key management system that is unique to each vehicle, making access to personal data subject to reliable user authentication techniques, etc.

The Guidelines particularly highlight security measures can be implemented by vehicle manufacturers: (i) partitioning the vehicle’s vital functions from those always relying on telecommunication capacities (e.g., “infotainment”); (ii) implementing technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle; (iii) setting up an alarm system in case of attack on the vehicle’s systems, with the possibility of operating in downgraded mode; (iv) storing a log history of any access to the vehicle’s information system, etc.

Conclusion

In February 2020, 22 ministries including the National Development and Reform Commission jointly issued the Intelligent Automobile Innovation Development Strategy\textsuperscript{30}. To accelerate

\textsuperscript{30} \url{http://www.gov.cn/zhengce/zhengceku/2020-02/24/content_5482655.htm}, the last visit: June 3, 2020.
the innovation and development of intelligent automobiles. Various local governments have also issued relevant local policies to implement the promotion strategy of the intelligent connected vehicle industry. Related laws and technical standards are also being formulated and improved. The issue of personal data protection in the context of connected vehicles is related to the basic rights and freedoms of individuals. Vehicle manufacturer and various service providers should all pay full attention to jointly establish a good personal data protection ecosystem of connected vehicles.

8. Eight Data Protection Key Words of Smart Home Launching out

Preamble

With the in-depth development of “Internet +”, the traditional home industry continues to explore new development paths and expand the “software-defined and integrated hardware” smart home route while update the hardware technology. At present, many domestic smart home manufacturers have aimed at overseas markets. As the smart home devices need to collect and process a large amount of data through smart cameras, smart speakers, etc. when providing services to users, the privacy and security issues of smart homes have gradually attracted public attention. In addition, global data protection legislation and law enforcement are becoming stricter, and more specific and stringent requirements are placed on personal data protection. Therefore, domestic smart home manufacturers should pay attention to personal data protection when expanding overseas markets. The personal data protection compliance has gradually become the standard configuration for products exported overseas.

This article is based on the requirements of General Data Protection Regulation (GDPR) compliance requirements, which constitute a complete overseas regulatory framework and set the most serious consequences for violations. Considering regulatory focuses, users’ concerns and industry practices, we have extracted eight smart home data protection keywords: informed, lawfulness, necessary, cooperation, security, cross-border, interaction, trend.

8.1 Keyword 1 Informed: How to ensure that users are fully informed and the requirements of transparency are meet?

According to the principle of transparency under GDPR, the personal data subject should be informed in a concise and easy-to-understand manner about their personal data processing before his/her personal data are processed.

---

Unlike ordinary web and APP products that can directly display privacy policies to users, smart home devices have the following typical difficulties when informing users: (i) for the content, the technical functions involved in smart home products are relatively complex, and the categories of personal data collected are complicated, making it relatively difficult for users to understand. (ii) for the form, some smart home devices do not have a screen and do not have voice interaction and other functions, and can only inform users through paper instructions and other methods. In order to provide users with complete and efficient services, some devices may be integrated into other devices and cannot make notifications independently. In addition, as a whole, the privacy policies of most domestic smart homes are currently of low transparency, and some important provisions are generally missing. If there are no timely corrections, the smart home device manufacturers will face great compliance risks when exporting smart homes overseas.

Considering the above difficulties, in order to ensure the realization of the user’s right to be informed and fully meet the requirements of transparency, companies can refer to the following ways to improve the product privacy policies: (i) for the content, manufacturers need to comprehensively sort out the product functions, and fully explain the personal data collected and processed for each function, the purpose of collection, whether it involves sharing, possible risks, etc. and appropriately explain the technical terms so that users can understand. (ii) for the form, smart home devices that can connect to App, have a display screen or a voice interaction, can inform users through the screens or voices. For products without the above functions, for one thing, manufacturers can instruct users to read the privacy policies in a prominent way on the product official website, or attach the privacy policies to the product introduction and documentation; for another, manufactures can add a QR code linking to the privacy policies on the products and prompt the user to read.


8.2 Keyword 2 Lawfulness: How to ensure that data processing activities have corresponding legal basis? Is the user’s consent necessary?

According to the principle of lawfulness under GDPR, all data processing activities must have an appropriate legal basis. According to Article 6 of GDPR, the legal basis mainly includes the consent of the data subject, the necessity to perform the contract, the necessity to perform the legal obligations, the protection of the interests of natural persons, the maintenance of public interest and legitimate interests.

For data processing activities carried out by smart home products, consistent with other products or services, it is necessary to determine the legal basis of the data processing activities. Generally speaking, the legal basis for companies to carry out data processing activities is mainly the user’s consent, the necessity to perform the contract and legitimate interests.

For data processing activities with legal basis of users’ consent (such as a smart bed that can monitor the health status of sleeping, heart rate, etc.; a smart door lock that uses fingerprints or face to unlock, and precision marketing, etc.), companies should pay attention that the valid consent should include six elements: freely given; specific; informed; unambiguous indication of wishes; the possibility to withdraw consent at any time and data controllers shall be able to demonstrate that the data subject has given his/her consent to the processing of his/her personal data. Companies shall obtain the consent of data subjects in line with the above requirements. For data processing activities with legal basis of necessity to perform contract (such as water heaters with automatic temperature control), companies should pay attention to improve the use terms of products or other user-oriented contract texts, covering the relevant descriptions of the data required to achieve the basic functions of the product, and ensuring that such collections do not exceed the minimum necessary scope for providing services based on the contract and do not exceed the reasonable expectations of users. For data processing activities with legal basis of legitimate

interests, companies need to conduct interest balance testing in a timely manner to ensure that appropriate organizational and technical measures have been taken to ensure that the realization of the business interests of the companies will not detract from the users’ basic rights and freedoms.

8.3 Keyword 3 Necessary: How to process personal data within the minimum necessary scope?

According to the principles of purpose limitation and data minimisation under GDPR, the collection and processing of personal data should have a specific and clear purpose and should only be processed within the minimum necessary scope to achieve the purpose.

Compared with other network products, the challenges faced by the data processing activities of smart home products to achieve the purposes mainly include: the Internet of Things (IoT) itself requires matching and comparison between multiple databases. Intelligent interconnection represents possible links to infinite potential activities, so it is necessary to judge whether the new function developed is a brand-new function or a reasonable extension of the existing function.\(^{36}\) Taking a smart sports watch as an example, the user agrees that the device collects data such as heart rate and movement trajectory for the purpose of monitoring its health status. If the company conduct automated decision analysis about the data and then sends targeted advertisements, it obviously exceeds the covered range of users’ consent.

In order to identify the possible risks and ensure that the data processing activities carried out by the smart home products fully meet the requirements of the principles of purpose limitation and data minimisation, the company should conduct a risk assessment, determine the implementation method of data minimisation based on the assessed results, and embed corresponding design in the entire life cycle of system development.\(^{37}\)

8.4 Keyword 4 Cooperation: How to manage personal data processing activities of cooperative third parties?

According to the smart home industry research report, with the continuous strengthening of integration between smart home platforms, nearly half of the devices can simultaneously access more than two smart interconnect platforms. At the same time, voice assistant service resources will continue to integrate. More smart home devices will be equipped with voice assistants.\(^{38}\)

---


Some smart home companies will choose to develop on smart home platforms such as Google home and Amazon Alexa when developing overseas markets, and use cloud-to-cloud technology control solutions to achieve voice control of devices. In this process, data interaction between three parties (users, smart home manufacturers, and smart home voice platforms) is involved and some manufacturers that only provide hardware and background O&M development may even involve data interaction between more than four parties. Therefore, it is necessary to fully clarify the rights and obligations of all parties, especially between manufacturers and platforms regarding data processing activities.

In practice, on one hand, companies must choose a platform with a high level of personal data protection compliance and information security ability for development, strictly follow various development agreements and requirements, and promote the signing of data processing agreements between relevant parties. On the other hand, it is necessary to continuously improve the research and development capabilities and the safety level of the equipment to avoid the situation where the cooperation platform secretly retains data for other purposes.  

8.5 Keyword 5 Security: How to ensure the security of personal data?

Smart home is based on a house, uses integrated wiring technology, network communication technology, security protection technology, automatic control technology, audio and video technology to integrate home life with related facilities, and build an efficient management system for residential facilities and family schedule affairs. Various devices or platforms are interconnected via Bluetooth, gateways, etc., and there is a greater risk of information security.

The information security risks faced by smart home products mainly come from three

---


aspects: Firstly, from external attacks, such as attacker destruction, data and identity theft, device hijacking, etc.\textsuperscript{41}. Secondly, from the device or the platform itself. For example, the device itself has not been fully tested for security before entering the market. There are obvious security holes or the back-end database has not been hardened, resulting in data breach, etc.; Lastly, from users themselves. Some users lack sufficient understanding of complex security technologies, leading to unaware of potential security risks.\textsuperscript{42}

Since some domestic smart home manufacturers were formerly traditional home appliance manufacturers, their experience and capabilities in information security are relatively weak. Based on the above risks and the actual situations, companies can start from the following points to continuously improve the ability to control security risk: strengthen information security capacity and security incident emergency response capabilities with high-level attention, resource input and personnel input, and apply for ISO 27001 and other information security certifications at the proper time; integrate security considerations from the product design and development stage, conduct full security testing of the products; and remind users of security risks through product descriptions, official website announcements, and connected Apps. .

8.6 Keyword 6 Cross-Border: How to transfer personal data to China in compliance?

According to Chapter V of GDPR, the cross-border transfer of personal data includes both physical transfers across national borders (referring to the physical transfer of personal data in terms of geographic location and space, including both transfers through the network and physical carriers for data to transfer personal data from a country/territory brought to another country/territory) and the situation where personal data is accessed remotely. When conducting cross-border transfer of personal data, it is necessary first to clarify the basic information of both parties and the jurisdiction where they are, and secondly to clarify the purpose and legal basis of the data transfer and ensure that there is an appropriate transfer.

\textsuperscript{43} “12 tips to help secure your smart home and IoT devices”, available at: https://us.norton.com/internetsecurity-iot-smart-home-security-core.html., the last visit: April 5, 2020,
security guarantee mechanism.

Based on the above regulations, when domestic smart home companies provide products and services to overseas users, whether they directly send data back to China, or set up a server locally or rent a cloud server for remote access by domestic personnel, the cross-border transmission of personal data will be involved.

For different means of data cross-border transfer, companies should take different compliance measures according to the actual situations. In the case of sending personal data directly from the product terminal or the local server back to China, for one thing, companies must fully inform users the privacy policies and obtain the consent of the personal data subjects when necessary; for another, companies can appropriately control the scale and frequency of the returned data in accordance with the actual needs of the business, and can take technical measures to encrypt, desensitize and anonymize the data. In the case of remote access, in addition to the description in the privacy policies and the consent of the personal data subjects if necessary, if it involves renting a third-party server, a data transfer agreement should be signed with these third parties, while limiting the scope and authority for personnel to access and authority for personnel to access and authority, etc. to avoid data security incidents.

8.7 Keyword 7 Interaction: How to protect users’ rights regarding personal data?

According to GDPR, data subjects enjoy the right to be informed, access, correct, delete, portability, object and restrict the processing. Data controllers or processors should have corresponding mechanisms to support data subjects to exercise their rights and make response to the rights request within the specified time.

Due to the characteristics of smart home products, they face the following difficulties in supporting the exercise of rights of personal data subjects. As mentioned in “keyword 1 Informed”, some smart home devices do not have screens and do not have voice interaction and other functions, and users have no easy way to exercise rights. In addition, because smart home products may involve the collection and processing of personal data of non-users, such subjects still have certain difficulties in exercising rights.44

In order to fully realize the rights of the data subjects, for products with screens or connected Apps, companies should set up corresponding functions for users to exercise their rights; for other products, they should be fully explained in the privacy policies, providing email, telephone and other methods to facilitate user to exercise rights. Within the company a complete data subject rights request response mechanism or procedure should be established and the corresponding technical capabilities should be improved to respond to user rights requests in a timely and efficient manner.

---

8.8 Keyword 8 Trend: What is the development trend of smart home personal data protection compliance?

According to Article 25 of GDPR, Privacy by Design refers to when deciding the purpose and method of data processing, appropriate organizational and technical measures should be considered and necessary security measures should be integrated in the process to realize the observance of the basic principles of data processing and the protection of the basic rights and freedoms of the data subject. Privacy by Default is to take appropriate organizational and technical measures to ensure that only necessary personal data is processed specific purposes by default. The two are collectively called Privacy by Design and Default (PbD). According to GDPR, all the requirements of PbD should be run through in the entire lifecycle of data processing activities, the basic principles of data protection should be fully implemented, and various compliance requirements should be fully considered at the initial stage of product development.

| Proactive not Reactive; Preventative not Remedial. | Privacy by Design is to proactively prevent issues before they occur, rather than seek reactively afterthought remedy. |
| Privacy as the Default Setting | Ensure that personal data is automatically protected in any given IT system or business practice. |
| Privacy Embedded into Design | Privacy by Design is embedded in the design and structure of IT systems and business practices. |
| Full Functionality: Positive-Sum, not Zero-Sum | Privacy by Design aims to satisfy all legitimate interests and purposes, rather than through a zero-sum method to balance interests and discard certain functions. |
| End-to-End Security: Full Lifecycle Protection | Before data collection, Privacy by Design should be embedded in the system and extend to the full lifecycle of the personal data involved to ensure privacy. |
| Visibility and Transparency: Keep it Open | Privacy by Design ensure that the operation of all relevant parties can be independently certificated, and is visible and transparent to users and product providers. |
| Respect for User Privacy: Keep it User-Centric | The purpose of Privacy by Design is to protect the basic rights and freedoms of individuals, and the measures taken should focus on respecting their privacy. |

The application of new technologies has triggered a series of personal data protection problems for smart home products, but it is also the key to solving these problems. More and more smart home manufacturers have begun to consider and embed PbD requirements at

---


the beginning of product design in order to reduce the privacy vulnerabilities of products and
the high cost of subsequent upgrades. When considering the integration of PbD requirements
into the full lifecycle of product design and data processing, companies can refer to the
following good practices: In the whole process, focus on the technical realization of data
pseudonymization and data minimization, while taking other organizational and technical
measures, such as encrypted transmission, encrypted storage, permission control, training
to enhance staff awareness and technical capabilities, etc. (For more recommendations
on the implementation of PbD requirements, please refer to our previous “5What is Data
Protection by Design and by Default—An Interpretation on EDPB Guidelines on Article 25
Data Protection by Design and by Default”.)

Conclusion

The development of 5G and artificial intelligence technology has promoted the development
and iteration of smart home products. While Chinese smart home companies continue to
explore overseas markets, they should also pay full attention to personal data protection and
compliance issues. On the basis of referring to the eight keywords in this article, companies
shall consider their oversea market planning, and gradually establish an internal personal
data protection system to create an external image of privacy protection, and make personal
data protection compliance capabilities a key competitive advantage and important booster
to develop overseas markets.
Cyber Security Law of the People’s Republic of China (CSL), which came into force on June 1, 2017, has established a core legal system for the cybersecurity and data compliance, covering rules for graded protection of cybersecurity, protection of critical information infrastructure, protection of personal information and important data, content management of information on the internet, management of cross-border data transfer. For the relationship of this law and other rule and regulations of People’s Republic of China, CSL, as a foundational and constructional legal document, has classified different sections and established principles for company’s cybersecurity and compliance work. In addition, it contributes the formation of an inclusive, malleable and adaptable operating rules.

With the continuous development in legislation and law enforcement activities, the structure of cybersecurity and data protection compliance system of People’s Republic of China has been being improved and the contents have been enriched all the time. A mature and effective regulatory system is forming gradually. This report has selected and generally introduced seven systems on which EU companies need to focus, when entering the Chinese market. We hope this report can serve as a basic guideline and help EU companies to achieve cybersecurity and data compliance in the China.

1. Rules on Personal Information Protection

1.1 Basic Content of Rules on Personal Information Protection
According to Article 76 of the Cybersecurity Law (CSL), personal information means all kinds of information recorded in an electronic or other forms, which can be used, independently or in combination with other information, to identify a natural person’s personal identity, including but not limited to the natural person’s name, date of birth, identity certificate number, biology-identified personal information, address and telephone number. According to Article 41 to 45 of CSL, network operators shall fulfill several requirements for personal information protection. These provisions have constituted the basis of the personal information protection system of China. In particular, article 41 provides the network operators’ obligation to inform subjects concerned and obtain their consent during and before the collection and use of personal information. Article 42 provides that network operators shall safeguard the security of personal information and Article 43 also sets obligations of network operators to safeguard the rights of personal information subjects.

Information Security Technology - Personal Information Security Specification ("Personal Information Security Specification") based on basic requirements of CSL and issued by National Information Security Standardization Technical Committee, has provided specific guidelines for the protection of personal information, as the main domestic standard for personal information full-life cycle management. Since the Personal Information Security Specification came into force in May 2018, several revisions have been made and two exposure drafts and one draft have been published in 2009. The latest edition has been released on March 6, 2020 and will officially come into force in October 1, 2020.

Besides, the Ministry of Public Security of the People’s Republic of China has released the Guidelines for Internet Personal Information Security Protection. The Guidelines, despite absence of compulsory binding force, have transformed the principled compliance requirements for the protection of personal information stipulated in the CSL into a management mechanism (management system, organization and personnel), technical measures and full-process management of personal information (collection, storage, application, deletion, sharing, disclosure, emergency response etc.). The protection on children’s personal information have been promoted with the promulgation of Provisions on the Cyber Protection of Children’s Personal Information as well.

In addition to the general requirements provided by CSL, Personal Information Security Specification and Guidelines for Internet Personal Information Security Protection, the processing of personal information in special industries (such as financial industry, map industry and credit industry) shall followed specific requirements for such industries. Therefore, EU companies shall follow not only the common requirements, but the specific requirements according to the specific industry oriented.

1.2 Law Enforcement Trend of Personal Information Protection

In January, 2019, the Office of the Central Cyberspace Affairs Commission, the Ministry
Implementation Guidelines on EU GDPR and Chinese Cybersecurity Law

of Industry and Information Technology, the Ministry of Public Security, and the State Administration for Market Regulation have jointly issued the Announcement of Launching Special Crackdown Against Illegal Collection and Use of Personal Information by Apps (“the Announcement”). In addition, a special working group against Apps collecting and using personal information in violation of laws and regulations has been established in association with relevant departments. The four ministries and commissions have taken the protection of personal information very seriously. With regard to problems such as the rampant collection of personal information through coercive permission, excessive requests of permission or beyond the approved scope, measures have been taken or will be taken to regulate these prominent issues which have caused grave concern for many people. On November 28, 2019, the special working group has formally issued the Method for Identifying the Illegal Collection and Use of Personal Information by Apps (“the Method”) to seek public comments. Followed the Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps (“the Guide”) issued in March 2019 by the special working group and combined the Personal Information Security Specification (“the Specification”) as well as serious violations of laws and regulations that frequently occur in the reporting activities, the Method reflects the focus of law enforcement agencies. It is of great reference significance for enterprises to evaluate compliance situation and set their own compliance red lines.

The comprehensive treatment which has lasted for one year have strengthened the punishment for illegal and unlawful activities and meanwhile matched the normative guidance and policy encouragement. The comprehensive measures are bound to solve prominent issues which have caused grave concern for many people, such as coercive permission, excessive requests of permission or beyond the approved scope, so as to achieve the expected regulatory effects of regulation of the App market. In 2020, the public security and network security departments shall continue the special rectification of illegal and unlawful activities of Apps, investigate and punish illegal collection and use of personal information in accordance with the law, and effectively protect citizens’ personal information and basic rights. In general, personal information protection law enforcement activities will be constantly strengthened and deepened. EU enterprises, when entering the Chinese market, shall fully consider the compliance of their personal information processing activities, avoid punishment and negative social impact.

1.3 Compliance Advice

In light of the current basic requirements under the personal information protection compliance system and the trend of law enforcement, EU enterprises, when entering the Chinese market, shall pay attention to the following compliance issues if personal information is involved in collection and processing. Extra attention shall be paid to fulfill the additional requirements set for information with relatively higher sensitivity such as personal sensitive information, biometric information.
<table>
<thead>
<tr>
<th>NO.</th>
<th>Activities</th>
<th>Fundamental Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Collection</td>
<td>Is there any explicit rules for collection and processing of personal information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Whether the means of presentation and the degree of detail of the rules for the collection and processing of personal information comply with the current laws and regulations regarding personal information protection and good practice in the industry</td>
</tr>
<tr>
<td>2</td>
<td>Collection</td>
<td>Whether the authorization and consent of the personal data subjects have been obtained</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Whether the requirements of authorization and consent are for different application scenarios and different categories of data (e.g., expressed consent requirement for the collection of personal sensitive information)</td>
</tr>
<tr>
<td>3</td>
<td>Collection</td>
<td>Whether channels and methods of collection are legal and compliant (especially in the aspects of delegate processing of data, data crawling and data fusion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Whether institutional and technical measures have been taken to ensure the legitimacy of data sources</td>
</tr>
<tr>
<td>4</td>
<td>Use/Processing</td>
<td>Whether the personal information collected is used faithfully in accordance with the requirements of laws and regulations and the agreement (on the rules of collection and processing of personal information) with personal information subjects and within the agreed scope</td>
</tr>
<tr>
<td>5</td>
<td>Use/Processing</td>
<td>Whether to compliance requirements have been fulfilled for application scenarios with higher compliance risks such as data fusion, analysis on user profile and marketing</td>
</tr>
<tr>
<td>6</td>
<td>Use/Processing</td>
<td>Whether there are unlawful or illegal activities such as illegally trading personal information</td>
</tr>
<tr>
<td>7</td>
<td>Management</td>
<td>Whether specific cyber security and data management organizations and persons in charge have been designated and granted with corresponding authorities and resources</td>
</tr>
<tr>
<td>8</td>
<td>Management</td>
<td>Whether the system for assessment of personal information have been established and perfected; whether the assessment work has been carried out on a regular basis</td>
</tr>
<tr>
<td>9</td>
<td>Management</td>
<td>Whether the rights of personal information of subjects as agreed provided by laws and regulations are guaranteed (right to access, right to correction, right to deletion of personal information, right to logoff, etc.) and whether operation in practice is consistent with the rules on collection and processing of personal information publicized</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>Is there proper control of internal and external access to personal information based on the principle of minimum sufficiency</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>Whether the corresponding technical measures have been taken to prevent personal information from being illegally copied, lost, damaged or stolen</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>Whether emergency response plans to cyber security and personal information incident have been formulated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Whether risk control measures have been taken and whether subjects concerned have been informed after the occurrence of incident and the countermeasures of supervisory authority been informed</td>
</tr>
</tbody>
</table>
### Implementation Guidelines on EU GDPR and Chinese Cybersecurity Law

<table>
<thead>
<tr>
<th>NO.</th>
<th>Activities</th>
<th>Fundamental issues</th>
</tr>
</thead>
</table>
| 13  | External Provision   | Whether the processing rules on external provision of personal information have been clarified  
|     |                       | Whether the means of external provision of personal information are safe and whether certain systems and technical protection measures have been taken  
|     |                       | Are relevant individuals informed of and consent to the security measures for the processing rules on external provision of personal information mentioned above  |
| 14  |                       | Whether a data processing agreement has been entered into with a third party to clarify the responsibilities and obligations of both parties in respect of data protection and compliance processing  |
| 15  |                       | Whether a cross-border transfer scenario is involved and whether the personal information involved is untransferable  
|     |                       | Whether the data recipients have evaluated the data protection capacity of the other party prudently  
|     |                       | Whether the personal data subjects concerned are informed of and consent to the cross-border transfer of their personal data |

In addition, the company shall progressively establish an internal personal information protection system, standardise collection and processing of various personal information carried out and provide basis for compliance of the processing of personal information. Besides, if companies’ major businesses are involved in the processing of personal information and their personnel number exceeds 200, or the amount of personal information involved is more than 1 million people or the processing involves the sensitive individual information of more than 100,000 people are, the company shall also specify persons responsible for personal information protection on full-time basis, as well as an organization for the protection of personal information. They shall be responsible for comprehensively planning and coordinating various work on personal information protection.

### 2. Multi-level Protection Scheme

#### 2.1 The Introduction to Multi-level Protection Scheme

Multi-level Protection Scheme (hereinafter referred as the “MLPS”) is a comprehensive management system for cybersecurity protection level assessment, filing and protection measures based on Article 21 of the CSL. Based on cybersecurity rating, the MLPS sets different standards of cybersecurity protection requirements for differed levels, covering organizational and personal arrangements, internal management system design and other organizational measures, as well as de-identification anonymization, encrypted storage and transmission, automated decision-making and recording, and other technical measures, providing quantitative standards and implementation paths for cybersecurity protection.
management set by the CSL. The network operators shall perform the cybersecurity protection compliance obligations in the company in consistence with the requirements of the CSL and the supporting system for the MLPS. If a network operators of corresponding system fails to implement the obligations of the MLPS, it will bear administrative liability for violating the explicit requirements of the CSL, and may bear civil liability to the data cooperative partner and relevant personal information subject in case of personal information breach or other security incidents caused by the system problem.

Starting with the Regulations of the People’s Republic of China on Protecting the Safety of Computer Information Systems issued in 1994 and revised in 2011, MLPS 1.0 is widely used in various industries to guide enterprises to carry out construction rectification, level assessment and other work of information system multi-level protection. The CSL, which was officially effective on June 1, 2016, stipulates the country implements MLPS, clarifying the legal status of MLPS, and also remarking the beginning of MLPS 2.0. On May 13, 2019, State Administration for Market Regulation and Standardization Administration issued the Information security technology—Baseline for classified protection of cybersecurity (GB/T 22239-2019, Baseline for classified protection), Information security technology —Evaluation requirement for classified protection of cybersecurity (GB/T 28448-2019) and Information security technology —Technical requirements of security design for classified protection of cybersecurity (GB/T 25070-2019). The three national standards in the field of cybersecurity came into effect on December 1, 2019, and jointly build MLPS in the new era, making the official arrival of MLPS 2.0. Besides, as one of the core standards in MLPS standard system, Information security technology—Classification guide for classified protection of cybersecurity (GB/T 22240-2020, Classification guide) was issued on April 28, 2020 and will be effective on November 1, 2020.

2.2 The Core Requirements of MLPS 2.0

(1) The Application Scope and Protection Objects

The application scope of the MLPS is society-wide, including but not limited to companies, government departments, public institutions and other legal persons and other organizations without legal person status like social organizations. Namely, except self-established and self-used networks of individuals and families, the application scope covers the whole society. The objects of the MLPS usually refer to systems composed of computers or other information terminals and related devices that collect, store, transmit, exchange, and process information according to certain rules and procedures, mainly including basic information network (refers to the network facilities and devices that play a basic supporting role such as information circulation and network operation, including telecommunication networks, radio and television transmission networks, the internet and private business networks, etc.), industrial control systems (such as on-site acquisition/execution system, on-site control system, process control system and production management system, etc.),
cloud computing platforms/systems (such as cloud computing platform, cloud computing infrastructure, related auxiliary service system, etc.), big data applications/platforms/resources, internet of things (such as systems that include perception, network transmission and other processing applications) and systems that use mobile internet technologies (such as mobile terminals, mobile applications and wireless networks) and so forth.

(2) The Basic Requirements for Safety Protection

According to Article 15 of the Regulation on Multi-level Protection (Draft for Comment), based on its importance to national security, economic development and social livelihood as well as its damage to national security, economic development, social livelihood and other organizations if it is destroyed, loses functions or encounters data leakage, from low to high, the cybersecurity protection can be divided into five levels from I to V. Different protection levels correspond to different foundational requirements for security protection capabilities.⁴⁷

• Level I

It shall be able protect the system from critical resource damage caused by malicious attacks from individuals, threat sources with few resources general natural disasters, and other threats of considerable harm and can be recovered after the system is damaged.

• Level II

It shall be able to protect the system from important resource damage caused by malicious attacks from small external organizations, threat sources with a small number of resources, general natural disasters, and other threats of considerable harm, and be able to discover important security vulnerabilities and security incidents, and recover some functions within a period of time after the system is damaged.

• Level III

It shall be able to protect the system from main resource damage caused by malicious attacks launched by externally organized groups, threat sources with rich resources, some serious natural disasters and other threats of considerable harm under a unified security strategy, and be able to discover security vulnerabilities and security incidents, and recover most functions quickly after the system is damaged.

• Level IV

⁴⁷ The Information security technology— Baseline for classified protection of cybersecurity (GB/T 22239-2019) notes: “The fifth level protection objects are very important regulating and management objects, which have special management modes and security requirements, so are not described in this standard.”
It shall be able to protect the system from the main resource damage caused by malicious attacks launched by externally organized groups, threat sources with rich resources, more serious natural disasters, and other threats of considerable harm under a unified security strategy, and be able to discover security vulnerabilities and security incidents, and recover most functions quickly after the system is damaged.

(3) The General Safety Requirements and Safety Expansion Requirements

The general safety requirements are divided into technical requirements and management requirements. The technical requirements specifically include a safe physical environment, a safe communication network, a safe area boundary, a safe computing environment and safe management center. The management requirements include safety management system, safety management organization, safety management personnel, safety management construction and safety operation and maintenance management. On the basis of the general requirements, different protection levels should meet the corresponding safety expansion requirements. In line with the increase of the level, the requirements of each control point shall increase level by level, the specific content is as follows:

<table>
<thead>
<tr>
<th>Level of Security Requirements</th>
<th>Cloud Computing</th>
<th>Mobile Internet</th>
<th>Internet of Things</th>
<th>Industrial Control System</th>
<th>Big Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level I</td>
<td>Safe physical environment; Safe communication network; Safe area boundary; Safe computing environment; Safe construction management</td>
<td>Safe physical environment; Safe area boundary; Safe computing environment; Safe construction management</td>
<td>Safe physical environment; Safe operation and maintenance management</td>
<td>Safe physical environment; Safe communication network; Safe area boundary; Safe computing environment</td>
<td>Safe communication network; Safe computing environment; Safe construction management</td>
</tr>
<tr>
<td>Level II</td>
<td>Added compared to level I: safe operation and maintenance management</td>
<td>The same as Level I</td>
<td>The same as Level I</td>
<td>Added compared to Level I; Safe construction management</td>
<td>Added compared to Level I; Safe physical environment; Safe operation and maintenance management</td>
</tr>
<tr>
<td>Level III</td>
<td>Added compared to Level II: Safe management center</td>
<td>Added compared to Level I and Level II: Safe operation and maintenance management</td>
<td>Added compared to Level I and Level II: Safe computing environment</td>
<td>The same as level II</td>
<td>The same as level II</td>
</tr>
<tr>
<td>Level IV</td>
<td>The same as Level III</td>
<td>The same as Level III</td>
<td>The same as Level III</td>
<td>The same as Level II and Level III</td>
<td>The same as Level II and Level III</td>
</tr>
</tbody>
</table>
(4) Classification and Assignment of Responsibilities

According to *Classification guide*, the general process of classification of the MLPS is divided into five steps: determination of classification objects-preliminary determination of the level-expert review-approval by the competent authority-review of the record. For objects whose security protection level is preliminarily determined as level II or above, the network operator shall organize expert review, approval by the competent authority and review of the record, within which:

- **Expert review**: the institutions who operate or use the classification objects shall organize information security experts and business experts to review the rationality of the preliminary classification results and issue expert review opinions.

- **Approval by the competent authority**: the institutions who operate or use the classification objects shall submit the preliminary classification results to the industry supervisor/regulator for approval and issues an approval opinion.

- **Public security bureau review**: the institutions who operate or use the classification objects shall submit the preliminary classification result to the public security bureau for record review in accordance with relevant management regulations. If the review fails, the institutions who operate or use the classification objects shall organize a re-classification; after the review is passed, the security protection level of the classification objects shall be determined.

In the work of the MLPS, the responsibilities of the companies and the competent authorities include:

<table>
<thead>
<tr>
<th>Step</th>
<th>Companies</th>
<th>Competent Authorities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification</td>
<td>Determine the objects of MLPS, determine the level of security protection, and prepare the classification filing materials.</td>
<td>Review whether the classification methods, working process, content, conclusions, etc. meet the regulations; organize experts to review the classification of the objects of the MLPS.</td>
</tr>
<tr>
<td>Filing</td>
<td>Prepare the filing materials and file with the cybersecurity department of the local public security bureau.</td>
<td>Accept the filing record, implement the record review and issue the certification.</td>
</tr>
<tr>
<td>Construction and Rectification</td>
<td>Carry out security technology and management system construction in accordance with national standards and industry standards of MLPS.</td>
<td>Organize experts to review the construction plan of the classification objects; review the security construction and rectification of the classification objects; implement a focused review the security construction of critical information infrastructure.</td>
</tr>
<tr>
<td>Classification Review</td>
<td>Regularly select qualified assessment institutions in the national recommended catalog for protection evaluation published by the Ministry of Public Security to carry out the assessment work.</td>
<td>Review whether the level assessment of the object of the MLPS conforms to the regulations; implement focused review of critical information infrastructure.</td>
</tr>
<tr>
<td>Supervision and Regulation</td>
<td>Accept and cooperate with the regulation and supervision of public security bureau and superior competent authority; regularly carry out security self-review.</td>
<td>Regularly conduct cybersecurity law enforcement regulation on the objects of the MLPS; implement protection for critical information infrastructure.</td>
</tr>
</tbody>
</table>
2.3 The Enforcement Tendency of the MLPS

China has increasingly strengthened the enforcement of cybersecurity violations. In 2018, the Ministry of Public Security organized 144,000 security inspections, found 1,346,000 security risks and management problems, and investigated and punished 34,000 internet companies. Take the case of a school in Anhui province which was punished for failing to perform obligations of the MLPS as an example. In August 2019, the school’s website was hacked and invaded due to the failure to implement the MLPS. When investigating the case, the cybersecurity detachment of the local public security bureau found that since the website was put into operation, the school had never carried out the work of classification record and review, failed to implement the obligations of the MLPS. The cybersecurity detachment of the local public security bureau imposed a fine on the school according to the law, and imposed a fine on the vice principal who was directly responsible.

In consideration of the serve situation of cybersecurity law enforcement, it is recommended that relevant companies should carry out the MLPS compliance work as soon as possible, establish internal management systems and security technical measures, set up corresponding management agencies and management personnel, and carry out a series of compliance works as classification, filing, assessment, rectification, etc.

2.4 Compliance Advice

In the process of entering the Chinese market, EU companies should take the protection measures in the following aspects to fulfill the obligations of the MLPS and avoid administrative punishments.

- Check whether your business involves operating cloud computing platforms/systems, big data applications/platforms/resources, the internet of things, and industrial control systems, etc. and promptly incorporate the above systems into the scope of protection work of the MLPS.

- Carry out compliance work of the MLPS as soon as possible, to determine the level, establish a management system, take technical measures, and actively fulfil various cybersecurity protection obligations.

3. The Critical Information Infrastructure Protection System

3.1 The identification of the Critical Information Infrastructures

The Critical Information Infrastructure protection system, based on the Article 31 to 39 of CSL, is a cybersecurity protection and regulation compliance requirement system for
the critical information infrastructure that will result in serious damage to state security, national economy and the people’s livelihood and public interest if it is destroyed, loses functions or encounters data leakage.

The CSL does not specify the detailed definition boundary and identification methods of Critical Information Infrastructure (hereinafter as “CII”). The corresponding Article 19 of the Regulation on Multi-level Protection (Draft for Comment) (the “Regulation on Protection”) also follows the Article 31 of the CSL, list the scope of CII with “non-exhaustive list + harmful consequences”, based on which companies can preliminarily assess whether their network systems shall be deemed as CII.

<table>
<thead>
<tr>
<th>Identification Contents</th>
<th>The CSL</th>
<th>The Regulation on Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>The industry and field to which the company belongs</td>
<td>Public communications and information services, energy, transportation, water conservancy, finance, public services, e-government and other important industries and fields</td>
<td>Government authorities and institutions in industries such as energy, finance, transportation, water conservancy, health care, education, social security, environmental protection, and public utilities, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information networks such as telecommunications networks, radio and television networks, the Internet, and institutions that provide cloud computing, big data, and other large public information network services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Scientific research and production institutions in the fields of national defense science and technology, large-scale equipment, chemical industry, food and medicine</td>
</tr>
<tr>
<td></td>
<td></td>
<td>News institutions such as radio stations, television stations, news agencies, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other important institutions</td>
</tr>
<tr>
<td>The harmful consequences caused by a cybersecurity incident</td>
<td>Serious damage to state security, national economy and the people’s livelihood and public interest if it is destroyed, loses functions or encounters data leakage.</td>
<td></td>
</tr>
</tbody>
</table>

Besides, to provide more specific guidance for companies, according to Article 19 of the Regulation on Protection, Cyberspace Administration of China will work with the State telecommunication department, the public security department and other departments to make the Identification Guidance of Critical Information Infrastructure (“Identification Guidance”). The national industry supervisors or regulatory authorities to which the CII belongs (such as Ministry of Industry and Information Technology of the telecommunication industry, National Energy Administration and National Development and Reform Commission of energy industry) will act in line with the Identification Guidance, organizing to identify CII in the industry and field, and submit the identification results according to the procedures. Before the Identification Guidance is published, the Operational Guidelines for National Cybersecurity Review (Operational Guidelines) made by Cyberspace Administration of
China in June 2016 has a strong reference value in CII identification process. According to *Operational Guidelines*, the judgment of CII can be made in consistent with the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Identification Contents</th>
<th>Identification Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>The first step</td>
<td>Identify the critical business</td>
<td>Analyze and identify whether the business of the infrastructure/system falls within the scope of businesses CII involves.</td>
</tr>
<tr>
<td>The second step</td>
<td>Identify information systems or industrial control systems related to critical business</td>
<td>Sort out information systems or industrial control systems that support or are related to critical business.</td>
</tr>
<tr>
<td>The third step</td>
<td>Refer to standards to identify CII from the importance of carrying business or severity of incidents.</td>
<td>Specifically assess whether any security incidents or damage to such information or control systems may lead to serious consequences, such as information breach that jeopardizes national security and public interests, interferes with normal operation of national economy, serious causalities or huge property loss.</td>
</tr>
</tbody>
</table>

### 3.2 The CII protection system

For the operators of CII (hereinafter as “CIIOs”), besides observing the general obligations of network operators, they should focus on compliance obligations for organization and management, security maintenance, and data protection of CII, including the requirement from Article 35 of the CSL to pass the state security review for procuring network products and services, the requirement from Article 36 of the CSL to enter into confidentiality agreements with network product and service providers, the requirement from Article 37 of the CSL to conduct security assessment for the storage and cross-border transfer of personal information and important data.

**1. The Cybersecurity Review**

According to Article 35 of CSL, where CIIOs purchase network products and services, which may affect state security, they shall pass the state security review organized by the national cyberspace administration in conjunction with relevant departments of the State Council. To further clarify the contents and procedures of security review, on 27th April 2020, the Cyberspace Administration of China together with 12 other bureaus, including the National Development and Reform Commission, jointly issued the *Measures for Cyber Security Review*, which replaces the *Measures for the Security Review of Network Products and Services (for Trial)*, will come into effect on June 1, 2020.

- The Scope of Review
When procuring network products and services, the CIIO shall prejudge the possible national risks to the country after the products and services are put into use. If it affects or may affect national security, the CIIO can make a security risk assessment report, and declare to the Cybersecurity Review Office, initiating the cybersecurity review. The network products and services mainly refer to core network devices, high performance computers and servers, mass storage devices, large databases and application software, cybersecurity device, cloud computing services, and other network products and services which have significant impact on the security of the CII.

For prejudgment of risk, the CII protection departments can make prejudgment guidance for specific industries and fields, to better guide CIIOs to prejudge the possible risks caused by the procurement of products and services.

• The Contents of Review

The cybersecurity review shall focus on national security risks that procurement of network products and services may bring, mainly including: The risks of illegal control, interference or damage to the Critical Information Infrastructure caused by the use of the products and services, and the theft, leakage and damage to the important data; The damage to business continuity of Critical Information Infrastructure caused by the disruption of the supply of products and services; The security, openness, transparency, source diversity of products and services, the reliability of supply channels and the risks of supply disruption due to political, diplomatic and trade factors, etc. Product and service providers’ compliance with Chinese laws, administrative regulations and departmental regulations; Other factors that may jeopardize the security of CII and national security.

• The Procedures of Review

The procedures of cybersecurity review can be generally divided into three steps:

The first step: sign a contract with the product and service provider, and the operator shall declare to the Cybersecurity Review Office for cybersecurity review and submit the following materials: the declaration, the analysis report on possible national security risks, the procurement documents, agreements, proposed contracts and other materials that cybersecurity review requires.

The second step: the Cybersecurity Review Office shall determine whether the review is needed within 10 working days after receiving the declaration materials and notify the operator in writing.

The third step: in case the Office of Cybersecurity Review deems it is necessary to conduct a cybersecurity review, it shall complete the preliminary review and reply its opinions
within 30 working days after notifying the operator in writing. In complicated situations, the review period can be extended by 15 working days. In case of the special procedures, the Cybersecurity Review Office shall form the review conclusion and notify the operator in writing within 45 working days. The review period can be extended in complicated situations.

- **Illegal Consequences**

According to Article 65 of the CSL, where a CIIO uses any network product or service that has not undergone security review or has failed to pass security review, the competent department shall order it to cease the use thereof, and impose a fine of not less than one time but not more than ten times the purchase amount on it, and impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on its directly responsible person in charge and other directly liable persons.

(2) **Data Localization and Data Cross-border Transfer Security Assessment**

According to Article 37 of the CSL, personal information and important data collected and produced by CIIOs during operations within the territory of the People’s Republic of China shall be stored within China. If it is indeed necessary to provide such information and data to overseas parties due to business requirements, security assessment shall be conducted in accordance with the measures developed by the national cyberspace administration in conjunction with relevant departments of the State Council, unless it is otherwise prescribed by any law or administrative regulation.

Though the *Measures on Security Assessment for Cross-border Transfer of Personal Information (Draft)* issued in 2017 expanded the obligation of data localization and security assessment to all network operators, it is not conclusive. For CIIOs, the implementation of the localization of important data and personal information and important data is a mandatory legal requirement and must be strictly followed.

3.3 **Compliance Advice**

For EU companies entering into Chinese market, it is extremely unlikely to be deemed as a CIIO, but a general network operator and a provider of network products and services. Therefore, we recommend:

When being deemed as a provider of network products and services, the company should actively cooperate with customers of CIIOs to conduct cybersecurity reviews, fulfill their security commitments to customers of CIIOs, and cooperate with supervisions and reviews. In the long run, it is also possible to gradually establish customer classification and project prejudgment mechanisms, establish a special process management mechanism for CIIOs to purchase projects, and perform special management on CIIOs.
When being deemed as a common network operator, the company should continue to pay attention to the relevant regulations on important data and personal information, and perform data localization obligations and conduct outbound security assessments in accordance with laws and regulations when necessary.

4. Rules on the Protection of Important Data

4.1 Identification of Important Data

The CSL does not provide the definition of important data. With the ongoing improvement of supporting regulations and norms, the provisions on the protection of important data have been becoming more and more clear by trend. Article 17 of the Measures for the Security Assessment of Personal Information and Important Data to be Transmitted Abroad (Exposure Draft)(“the Measures for the Assessment”) formulated in 2017 has defined important data as data closely related to national security, economic development, and social and public interests. Subsequently, the National Information Security Standardization Technical Committee have raised in the Guidance on the Identification of Important Data in the Information Security Technology - Guidance on the Security Assessment of Cross-border Data Transfer issued on August 25, 2017. And the Guidance on the Identification of Important Data has pointed out that important data refers to data (including primary data and derivative data) that is collected and generated by the relevant organizations, institutions and individuals within the territory of the People’s Republic of China, which does not involve state secrets but is closely related to national security, economic development, social and public interests. Once the data is disclosed, lost, misused, tampered with or destroyed, or is gathered, integrated and analyzed without authorization, severe consequences may be caused. Also, the Guidance on the Identification of Important Data has listed the scope of important data involved in each industry and field. Article 38 of the Administrative Measures on Data Security (Exposure Draft) formulated on May 28, 2019 has defined important data in more detail way, stating that “Important data” refer to the kind of data, if divulged, may directly affect national security, economic security, social stability and public health and security, such as undisclosed government information, large-scale population, genetic health, geography and mineral resources, etc. Important data shall usually not include information related to the production and operation and internal management of enterprises or personal information, etc. Therefore, in addition to the general statement, the Measures enumerate some examples and explicitly exclude the possibility that the information on production, operation and internal management as well as personal information of an enterprise may be taken as important data. However, it also can be seen that the Measures still do not provide for the specific method for the identification of important data.

4.2 Protection of Important Data
In accordance with *the Administrative Measures on Data Security (Exposure Draft)*, the collection, use and cross-border transfer of important data are subject to the corresponding requirements. The requirements include:

Network operators shall make a filing with the local cyberspace administration when they collect important data or sensitive personal information for the purposes of business operations. The filing shall include the rules for collection and use of such data, purposes, scales, methods, scopes, types and retention periods of the data, but shall not include the contents of data themselves. Meanwhile, network operators shall specify the persons responsible for data security.

Network operators shall, when using important data, take technical measures such as data categorization, data backup and encryption to strengthen the protection of personal information and important data.

Network operators shall assess the potential security risks prior to releasing, sharing or selling important data or transferring such data abroad, and shall report to the competent regulatory department for approval. If the competent regulatory department is unclear, network operators shall report to the cyberspace administrations at the provincial level for approval. On June 13, 2019, the Cyberspace Administration of China issued *Comments on the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment)*. Compared with the requirements set forth in *the Measures for the Assessment* for the assessment of the transfer of “personal information” and “important data”, *the latest version of the Measures for the Assessment* only set out relevant provisions on the assessment of the transfer of “personal information”. Therefore it can be seen that the regulatory department intend to separate the administration of the transfer of important data and personal information and apply different regulatory principles.

In addition, if any critical information infrastructure operator is constituted, the storage of important data requirements shall comply with localization requirement; if it is indeed necessary to provide any data to overseas parties due to business needs, a security assessment shall be conducted in accordance with the measures formulated by the cyberspace administration of China in concert with relevant departments under the State Council.

### 4.3 Compliance Advice

As there is no standard for the identification of important data in respective industries for the time being, the specific identification or determination methods for important data are not clear. Therefore, dynamic analysis and comprehensive judgment are also required in terms of whether data to be transferred abroad is important data. For Chinese enterprises entering EU market, it is advised to pay continuous attention to *the Administrative Measures*
on Data Security (Exposure Draft), standards of relevant industries, guides and other latest legislative status of relevant laws and regulations concerning important data. If it is determined later that the data to be transferred abroad falls within the scope of important data, relevant strategies and measures shall be adjusted in a timely manner. For example, prior to the cross-border transfer, your company shall go through appropriate procedures such as carrying out assessment, seeking registration and approval from the supervisory authority, in accordance with effective laws and regulations.

5. Internet Real Name System and Regulation on User Information Release

5.1 Internet Real Name System

(1) Legal Requirements

The Cyber Security Law of the People’s Republic of China (CSL), which came into force on June 1, 2017, sets specific requirements for the Internet Real-Name System according to Paragraph 1 of Article 24 of CSL, where network operators provide network access and domain registration services for users, handle network access formalities for fixed-line or mobile phone users, or provide users with information release services, instant messaging services and other services, they shall require users to provide true identity information when signing agreements with users or confirming the provision of services. If any user fails to provide his or her true identify information, the network operator shall not provide him or her with relevant services. Article 13 of Provisions for the Administration of Internet News Information Services, which is effective since June 1, 2017, also provides that An Internet news information service provider that provides users with Internet news information dissemination platform services shall request users to provide authentic identity information. An Internet news information service provider shall not provide relevant services for any user that does not provide authentic identity information. Meanwhile, with the promulgation of regulatory documents such as the Provisions on the Administration of Internet Comments Posting Services, Provisions on the Administration of Internet Live-Streaming Services, Provisions on the Administration of Internet Group Information Services and Provisions on the Administration of Internet Forum and Community Services, requirements for Internet Real Name System have becoming more and more specified and strict.

In addition, the Interpretations of the Supreme People’s Court and the Supreme People’s Procuratorate on Several Issues concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to Information Network issued on October 21, 2019 has further explained the provisions on the crimes as refusing to perform the obligation of safety management for information networks, illegally using an information network and providing aid for criminal activities in relation to information networks. For the crime of
refusing to perform the obligation of safety management for information networks, those failing to retain a vast majority of user logs or perform the obligation of identifying the authentic identity information shall be deemed “falling under other serious circumstances” prescribed in item 4, paragraph 1, Article 286(I) of the Criminal Law and the criminal suspect or defendant may be sentenced to imprisonment of not more than three years, supervision without incarceration, limited incarceration in addition to a fine, or be sentenced to a fine only.

(2) Law Enforcement Trend

With the gradual improvement of relevant provisions, regulations, the law enforcement activities for the Internet Real-name System have become increasingly stringent. In the “Net-Network 2019” national special action of the Cyber Security Bureau of the Ministry of Public Security, all local public security and communication management departments have actively taken regulatory actions, and listed the implementation of the real-name registration information of the Internet enterprises as the focus of administrative law enforcement. For example, Beijing public security organs have released typical law enforcement for companies on failure to implement the real-name registration; Guangdong Communications Administration has carried out intensive actions to implement the internet real-name system, cleaned up and removed more than 151,000 applications fail to fulfill real names requirements; Hubei public security organs have cleaned up and removed 2092 applications that fail to fulfill real names requirements or those conducted illegal or irregular activities. After the Cyber Security Bureau of the Ministry of Public Security officially launched the special action of “Net-Network 2020”, the Internet Real-Name System still remains the focus of regulation.

Take the case that the Office of Cyberspace Affairs Commission interviewed the website involved in Li Wenxing incident and ordered a immediate rectification on the direct recruitment App for example, Li Wenxing, a graduate of Northeastern University, by using the direct recruitment App, got involved in the deadly incident of pyramid sales organization. This incident aroused widely concern from the public. The Office of Cyberspace Affairs Commission of Beijing in concert with the Office of Cyberspace Affairs Commission of Tianjin had an interview with the principal of the company; upon investigation, this App was found to provide information release service for the users who have not provide real identity information authentication, which violates relevant regulations; besides, this App failed to take effective measures to strictly manage the information released and transmitted by the users, resulting in the spread of information in violation of laws and regulations; therefore, the App was ordered to immediately conduct self-inspection and rectification.

Failure to perform the obligations under the real-name requirements is not only a violation of the statutory obligations provided in the Cyber Security Law, but also is likely to cause adverse influence on the public and lead to violation of laws and crimes. EU companies
wishing to enter the Chinese market, especially those provide information release services and instant messaging services, shall ensure the performance of various obligations including the real-name requirements, and at the same time, pay attention to relevant qualification issues. In addition, to find out whether the fields they engaged are open for foreign investment and relevant requirements thereof.

5.2 Regulation on User Information Release

(1) Statutory Requirements

According to Article 17 of CSL, Network operators shall strengthen the management of information released by their users. If any operator finds any information of which the release or transmission is prohibited by any law or administrative regulation, it shall immediately cease the transmission of such information, take deletion or any other handling measure to prevent the information from spreading, preserve relevant records, and report it to the competent department. Laws and regulations such as Counterterrorism Law of the People’s Republic of China, Public Security Administration Punishments Law of the People’s Republic of China, Administrative Measures for Internet Information Services and Interim Provisions on the Administration of Internet Culture have explicitly stipulated categories of information that shall not be distributed or published, including but not limited to information against the Cardinal Principles set forth in the Constitution; detrimental to State security, State secrecy, State power and national unification; detrimental to State religious policy, propagating heretical or superstitious ideas; disseminating rumours, disrupting social order and stability; disseminating obscenity, pornography, force, brutality and terror or crime-abetting and so on.

Came into force since March 1, 2020, the Provisions on Ecological Governance of Network Information Content ("the Provisions") defines the rights and responsibilities of subjects as network information content producers, network information content service platform, internet industry organizations, supervisory and regulatory authorities such as the cyberspace authorities at all levels. In addition, the Provisions also defines ten red lines that network information content producers shall not touch and eight types of bad information that network information content producers shall prevent and resist.

In order to achieve the important spirit and key objectives of “comprehensively improving the network governance capacity and creating a clear cyberspace”, it is necessary to regulate network information content, establish a good network ecology, carry forward positive spirits, and deal with illegal and bad information.

(2) Law Enforcement Trend

Since January 2019, the Office of the Central Cyberspace Affairs Commission has begun the
special program for the governance of cyber ecology that lasts for six months to deal with twelve types of negative and harmful information, including the obscene and pornographic information, vulgar information, violent and bloody information, horror, gambling fraud, online rumors, feudal superstition, verbal abuse and spoof, threat and intimidation, clickbait, hate incitement, dissemination of harmful lifestyles and bad pop culture. The special program mainly concentrates on dealing with key issues of cyber ecology. By making full use of existing administrative law enforcement measures, a number of illegal websites and accounts have been severely investigated, punished and closed in order to actively respond to people’s concerns and promote cleaner cyber ecological space.

On May 11, 2018, at 20:03, Ergeng’s official wechat account, “Ergeng Canteen”, published a vulgar article and misdescribed a hitchhiker’s personal injury incident, triggering strong revulsion among Weibo and WeChat moments. Therefore, the Internet Information Office of Zhejiang Province and the Internet Information Office of Hangzhou interviewed “Ergeng Canteen”. This act violated provisions of Administrative Measures for Internet Information Services, broke through the “seven bottom lines”, deviated from the orientation of socialist core values and destroyed the normal network communication order. In response, the Zhejiang Cyberspace Administration Office and the Hangzhou Cyberspace Administration Office quickly conducted an interview with the person chiefly in charge of the WeChat public account, and required comprehensively cleaning up on illegal and harmful information, seriously punishing the relevant persons liable and submitting rectification reports within a prescribed time limit. Meanwhile, the official account of “Ergeng Canteen” has been blocked by the WeChat platform for seven days.

In order to achieve the important spirit and key objectives of “comprehensively improving the network governance capacity and creating a clear cyberspace”, it is necessary to regulate network information content, establish a good network ecology, carry forward positive spirits, and deal with illegal and bad information. Therefore, when EU companies carry out business in the Chinese market, if they fulfill relevant qualification requirements and allow users to post the relevant information on their websites, they shall establish a user information management system and strictly examine the information released by users. Also, when using the public platform for publicity, EU companies shall also pay attention to the requirements of the relevant provisions, strictly resist unfavorable information, and shall not break the law.

6. The Network Product and Service Management System

The legal requirements in China for network products and service providers are mainly divided into two aspects: one is to regulate network products and services themselves, including legal requirements for common network products and services and special products like key network equipment and specialized cybersecurity products for cybersecurity; the
other is to set corresponding legal obligations for different entities to purchase network products and services, such as CIOs.

6.1 Network Products and Services Themselves

(1) Common Network Products and Services

According to Article 22 of the CSL, the provider of common network products and services shall ensure: the related network products and services comply with the compulsory requirements of relevant national standards; The network products and services do not contain malware. When a provider discovers any risk such as security defect and vulnerability of its network products or services, it shall immediately take remedial measures, inform users in a timely manner, and report it to the competent department in accordance with relevant provisions. The provider can continuously provide security maintenance for their products and services, and shall not terminate the provision of security maintenance within the stipulated period or the period agreed upon by the parties; If network products and services have the function of collecting users’ information, their providers shall explicitly notify their users and obtain their consent. If any user’s personal information is involved, the provider shall also comply with this Law and the provisions of relevant laws and administrative regulations on the protection of personal information.

(2) Key Network Equipment and Specialized Cybersecurity Products

According to Article 23 of the CSL, Key network equipment and specialized cybersecurity products shall, in accordance with the compulsory requirements of relevant national standards, pass the security certification conducted by qualified institutions or meet the requirements of security detection before being sold or provided. The national cyberspace administration shall, in conjunction with relevant departments of the State Council, develop and release the catalogue of key network equipment and specialized cybersecurity products, and promote the mutual recognition of security certification and security detection results to avoid repeated certification and detection. In 2018, Certification and Accreditation Administration of China issued the Rules for Implementing Key Network Equipment and Specialized Cybersecurity Products Security Certifications, which comprehensively stipulates the scope, certification model, basic steps for certification, certification implementation, certification time, certificate, etc. regarding key network equipment and specialized cybersecurity products, and proposes the “Key Network Equipment and Specialized Cybersecurity Products Catalog”.

(3) Special Products for the Safety of Computer Information Systems

According to Article 3 of the Measures for the management of test and sale license of Special Products for the Safety of Computer Information Systems, the sale license system shall
apply to special products for the safety entering into Chinese Markets. Before the special products enter the markets, the provider shall apply the Sale License of Special Products for the Safety of Computer Information Systems. Therefore, if your company provides special products for the safety of computer information systems, you should ensure you have obtained the sale license for the products.

Besides, according to the requirements of CII protection system mentioned above, information system operators at and above level III should follow the corresponding requirements in the selection and procurement of information security products.

(4) Cryptographic Products

For the related requirements of cryptographic products, please refer to the specific content of cryptographic product management system in Section 7 of this part.

6.2 The Procurement of Network Products and Services by Customers

When network products and services purchased by a CIIO involving national security, the provider of network products and services shall cooperate for the cybersecurity review and sign the confidentiality agreement. Please see the details in Section 3 of this part regarding CII protection system.

6.3 Compliance Advice

For EU companies entering Chinese market, in order to meet the requirements for different types of products and services, they shall firstly identify the type of products and services they provide, and then follow the corresponding requirements for common network products and services, key network equipment, specialized cybersecurity products, special products for the safety of computer information systems, and cryptographic products. Moreover, they should classify their customers, and perform corresponding obligations for special type of customers.

7. The Cryptographic Product Management System

7.1 A Brief Introduction to the Cryptographic Product Management System

On October 26, 2019, the 14th session of the Standing Committee of the 13th National People’s Congress passed and promulgated the Cryptography Law of the People’s Republic of China (hereinafter referred to as the “Cryptography Law”) which shall be effective as of January 1, 2020.
Prior to that, the rules of high legislation hierarchy on cryptography administration could be traced back to the *Regulations on the Administration of Commercial Cryptography* (hereinafter referred to as the “Regulations”) promulgated by the State Council in October 1999. Thereafter, the State Cryptography Administration and the Standing Committee of the National People’s Congress promulgated the *Cryptography Law of the People’s Republic of China (Draft for Comment)* and the *Cryptography Law of the People’s Republic of China (Draft)* (hereinafter referred to as the “Cryptography Law (Draft)”) respectively on April 2017 and July 5, 2019. The *Cryptography Law* which is based on the *Cryptography Law (Draft)* and has improved the same fills the long-standing legal gap in the field of cryptography and is the first comprehensive law on cryptography administration in our country.

(1) The Applicable Objects of Cryptographic Product Management System

The applicable object and supervision target of the *Cryptography Law* is cryptography, which is not limited to cryptographic products and technologies, but also includes cryptographic services. It should be pointed out that the cryptography in the *Cryptography Law* is not exactly the same as the “cryptography” mentioned in our daily life. The “cryptography” that is often encountered in life is only the password or “passport” for entering personal devices or software, which is a primary means of identity authentication. However, the cryptography in the *Cryptography Law* refers to technology, product and service that effect encryption protection or security certification of information and the like by adopting the method for specific conversion, whose function is reflected encryption protection or security certification of information, through the method for specific conversion.

(2) The Classification of Cryptography

Today, with the rapid development of informatization and digitalization, the application of cryptography can be found in all aspects of national economy and social life. It has gradually become a shield and strategic resource to safeguard national cyberspace sovereignty, security and development interests. Due to the fact that different cryptography is used to protect different objects, in order to fully enable the core supporting role of different cryptography in protecting cybersecurity and information security, the *Cryptography Law* implements classified management of cryptography, and defines the classification level of cryptography. In descending order of the confidentiality level of the information to be protected, the classification levels of cryptography are core cryptography, ordinary cryptography and commercial cryptography. The management and use of each cryptography are provided under corresponding chapters in the *Cryptography Law* which makes the legislative style and the application of laws clearer and more scientific.

The *Cryptography Law* expressly stipulates that core cryptography and ordinary cryptography are state secrets. Commercial cryptography is used to protect information that is not a state secret and the commercial cryptography itself is not a state secret. The highest
confidentiality level of the information protected by core cryptography is top-secret level. Therefore, core cryptography can be used to protect the information that is of top-secret level, secret level and confidential level. The highest confidentiality level of the information protected by ordinary cryptography is the secret level. Therefore, ordinary cryptography can be used to protect the information that is of secret level and confidential level. The commercial cryptography is used to protect information that is not a state secret. Citizens, legal persons and other organizations may use commercial cryptography to protect cybersecurity and information security in accordance with the laws.

7.2 “Regulation” and “Deregulation” Under the Cryptography Law

(1) “Deregulation” Under the Cryptography Law

In order to implement the reform requirements to “delegate power, streamline administration and optimize government services”, since the Cryptography Law takes effect, competent authorities have been actively stipulating supporting rules to implement the “deregulation” under the Cryptography Law. To be more specific:

• On September 29, 2017, the State Council issued the Decision on Cancelling a Number of Administrative Licensing Items (Guo Fa [2017] No. 46), cancelling the following four administrative licensing items that were implemented by the State Cryptography Administration: the approval for commercial cryptographic product manufacturers, the licensing for commercial cryptographic product sellers, the approval for the use of foreign-produced cryptographic products by foreign-invested enterprises, and the approval for use of cryptographic products or the equipment containing cryptographic technologies in China by foreign organizations and individuals.


• On December 30, 2019, the State Cryptography Administration and the State Administration for Market Regulation issued the Announcement on Adjusting the Management Methods of Commercial Cryptographic Products (“Announcement No. 39”), which abolished the “approval system by way of model certificate for commercial cryptographic products” and
established the certification system to be uniformly adopted throughout the whole nation. The State Cryptography Administration no longer issues Model Certificate for Commercial Cryptographic Products as of January 1, 2020, and the existing Model Certificates cease to be effective as of July 1, 2020. Under the certification system regimes, commercial cryptographic products that are not listed under the Catalogue of Critical Network Equipment and Dedicated Cybersecurity Products shall be subject to the certification system on a voluntary basis and the production and sale of which is no longer subject to the Model Certificate for Commercial Cryptographic Products.

The promulgation of the Cryptography Law marks the formal cancellation at the state legislation level of the following approving and licensing implemented by the State Cryptography Administration: the approval for commercial cryptographic product manufacturers, the licensing for commercial cryptographic product sellers, the approval for the use of foreign-produced cryptographic products by foreign-invested enterprises, and the approval for use of cryptographic products or equipment containing cryptographic technologies in China by foreign organizations and individuals. The administration on the production and sale of commercial cryptographic products is being loosened as well.

However, it should be noticed that the cancellation of the above administrative approvals does not imply a complete liberalization of administration by the state on use of cryptography, but rather signals that the regulatory focus is shifting from “administering entities” to “administering products”. Whereas how the products would be administered is subject to further implementation by the State Cryptography Administration, the State Administration for Market Regulation, Ministry of Commerce and the General Administration of Customs:

Under the certification system regime provided under Announcement No. 39, the sale or supply of commercial cryptographic products that are listed under the Catalogue of Critical Network Equipment and Dedicated Cybersecurity Products shall be subject to the mandatory certification by qualified testing and certification agencies.

According to the Notice of the State Cryptography Administration on the Transition of Relevant Administrative Policies after the Cancellation of Four Administrative Licenses including the Examination and Approval for Manufacturers of Commercial Cryptographic Products (Guo Mi Ju Zi [2017] No. 336, “Notice No. 336”) issued on October 11, 2017, enterprises selling commercial cryptographic products shall continue to comply with the requirements of the record-filing system for the sale of commercial cryptographic products. Whether such a record-filing system would remain in force after the approval system by way of model certificate for commercial cryptographic products is abolished is to be further clarified by the competent authorities.

In addition, if the cryptographic products or equipment containing cryptographic technology
used by foreign-invested enterprises, foreign organizations and individuals need to be imported from abroad, the *Import License for Cryptographic Products and Equipment Containing Cryptographic Technology* shall still be obtained according to the laws and regulations, and the importer shall disclose the end user and end use of the imported cryptographic products when importing them. According to the *Announcement No. 38 by the State Cryptography Administration, Ministry of Commerce and the General Administration of Customs* (“Announcement No. 38”) issued on 30 December, 2019, such import license system would remain in place till the import-license-export-control-list system is put into practice.

(2) “Regulation” Under the Cryptography Law

It is obvious that the regulation practice on commercial cryptography mentioned above reflects that the focus of the regulatory authorities with respect to cryptography administration has shifted from ex ante approval to interim and ex post regulation. At the same time, the supervision department is implementing the “regulation” through the following regulatory structure design, which manifests the attitude of the regulatory bodies that neither “regulation” or “deregulation” is being neglected. It is important to ensure that both “regulation” and “deregulation” of cryptography administration are being enforced simultaneously.

• Import-license-export-control-list system

In consistence with internationally recognized practice, the Ministry of Commerce and the State Cryptography Administration implement a list-based administration system for the import and export of commercial cryptography, that is, an import-license-export-control-list system will be implemented for commercial cryptography with the encryption protection functions that involves national security and public interest. This is of great significance to prevent the use of commercial cryptography to commit illegal criminal activities. By the time the *Cryptography Law* entered into effect, the implementing rules on the import-license-export-control-list system had not been published yet. For the transition period till the list is issued, the Ministry of Commerce, the State Cryptography Administration and the General Administration of Customs made the following arrangements in the *Announcement No. 38*: (1) for import of the cryptographic products or equipment containing cryptographic technology, *Import License for Cryptographic Products and Equipment Containing Cryptographic Technology* shall still be obtained under the existing regulatory regime, (2) for export of commercial cryptographic products, service providers shall apply to the state and local cryptography administrations for approval of commercial cryptographic products export and obtain an *Export License for Commercial Cryptographic Products*.

• Testing and certification system of commercial cryptographic products and services

According to the *Cryptography Law*, commercial cryptographic service used for critical
network equipment and dedicated cybersecurity products shall be subject to the mandatory testing and certification system; other commercial cryptographic service providers shall be subject to the voluntary testing and certification system. The provisions that subject testing and certification of commercial cryptographic products to the *Cybersecurity Law of the People’s Republic of China* (hereinafter referred to as the “CSL”) reflect the connection and coordination between the *Cryptography Law* and the CSL.

The *Cryptography Law* imposes the compulsory testing and certification system only on commercial cryptographic products involving national security, national people’s livelihood and social public interests and commercial cryptographic services used in the critical network equipment and dedicated cybersecurity products. Additionally, the competent department in practice will define the scope of its administration by issuing and timely updating the Catalogue of Critical Network Equipment and Dedicated Cybersecurity Products. In this way, the administration of commercial cryptography is facilitated by a standardized testing and certification system while a balance between the administration and the development of the cryptography industry could be maintained.

According to the *Announcement No. 39*, the State Administration for Market Regulation and the State Cryptography Administration would at another time promulgate a product catalogue for commercial cryptographic products certification, certification rules and pertinent implementing requirements. On February 20, 2020, the State Administration for Market Regulation published the *Implementation Opinions on Carrying out the Testing and Certification Work of Commercial Cryptographic Products (Draft for Comment)*. If the draft enters into effect as it is, the product catalogue for commercial cryptographic products certification would be issued jointly by the State Administration for Market Regulation and the State Cryptography Administration, the certification rules would be issued by the State Administration for Market Regulation, and the qualification of testing and certification agencies would be subject to the approval by the State Administration for Market Regulation.

- Security assessment and national security review of the cryptography applications procured by Critical Information Infrastructure Operators

The *Cryptography Law* stipulates the corresponding control measures for the products that involves national security, the national economy and people’s livelihood, social and public interests, that are listed in the catalog of critical network equipment and dedicated products for cybersecurity, as well as the purchase of products and services by the operators of critical information infrastructure (hereinafter referred to as “CIIO”). It reflects the balance between the reform requirements to “delegate power, streamline administration and optimize government services” and the protection of national security. From the relevant provisions of the *Cryptography Law*, it is obvious that it correlates with the *Cybersecurity Law, Regulations on the Security Protection of Critical Information Infrastructure (Draft for comment), Measures for Cybersecurity Review* and other laws and regulations. In addition,
the *Cryptography Law* also coincides with relevant provisions of the *Regulations on the Multi-Level Protection Scheme for Cybersecurity (Draft for Comment)*. For example, a network at or above Level III shall adopt cryptographic technologies, products and services recognized by the state cryptography administrations, and an institution shall be entrusted to evaluate the security of cryptography applications, and the result thereof shall be filed with the competent authority concerned for the record.

### 7.3 The Equal Market Participation Position of Foreign Investment in the Field of Cryptography

The *Cryptography Law* provides that foreign-invested enterprises engaged in the research, production, sales, service, import and export of commercial cryptography must be treated equally. From the time when the State Cryptography Administration cancelled most of the administrative approvals in 2017, to the further market opening by the *Cryptography Law*, foreign-invested enterprises are treated equally with domestic enterprises in China, specifically:

- **No prior approval is required** before foreign-invested enterprises produce, sell and use domestic commercial cryptographic products in China. Yet, if the commercial cryptographic product is listed under the Catalogue of Critical Network Equipment and Dedicated Cybersecurity Products, it shall be tested and certified by qualified agencies.

- Foreign-invested enterprises may on a voluntary basis apply for commercial cryptographic product certification via the prescribed process to be published by the State Administration for Market Regulation if the commercial cryptographic product is not listed under the *Catalogue of Critical Network Equipment and Dedicated Cybersecurity Products*.

- **For the import of foreign-produced cryptographic products and equipment** with cryptographic technology, it is still necessary to obtain the *Import License for Cryptographic Products and Equipment with Cryptographic Technology* till the import-license-export-control-list system is put into practice.

In addition, in response to foreign investors’ concerns about mandatory technology transfers, there are specific regulations prohibiting the mandatory transfer of commercial cryptographic technologies in the *Cryptography Law*. These provisions are the reflection in the cryptography administration of the principle of prohibiting compulsory technology transfer which is set by the *Foreign Investment Law of the People’s Republic of China* promulgated in March 2019. These rules are in favor of protecting the rights and interests of foreign investors and stimulating the investment enthusiasm of foreign-invested enterprises.

In general, the promulgation of the *Cryptography Law* promotes fair competition in the market for the foreign-invested enterprises.
7.4 Compliance Advice

Being the first fundamental law in the field of cryptographic administration, the *Cryptography Law* will improve the scientific and standardized administration of cryptography, and will also promote the cryptographic technology progress, industrial development and standardized application of cryptography. It is expected that the vigorous development of the cryptographic industry will bring new opportunities to companies.

For EU companies entering Chinese market, as mentioned above, the promulgation of the *Cryptography Law* will help foreign companies to enter the market competition fairly. Foreign investors can make full use of this benefits, to find their own value proposition, and actively conduct business with Chinese companies for cooperation in commercial cryptography and develop related markets jointly.

Disclaimer

Any content of this report is for recommended reading or reference only and is not intended to and does not constitute any legal advices or views of Zhong Lun Law Firm. The authors of this report, and the agents thereof undertake no liability and give no warranty in relation to any likely consequences arising from the use of any information in this report. The authors reserve all rights to this report. No individual shall, in any form or by any means, reproduce any copyright content in this report, without written permission from the authors. For more information about this report, or if you have any comments and suggestions, please contact the authors.
Wolters Kluwer is a leading global information services and solutions company. It provides information, software, and services that help legal, tax, finance, and healthcare professionals make their most critical decisions effectively and with confidence. Customers depend on Wolters Kluwer services and solutions to successfully move through the complex layers of data and regulation that define modern business and government.

Wolters Kluwer entered Mainland China in 1985. Depending on global connections and experience as well as dedication to local markets and client needs, Wolters Kluwer is able to provide timely, accurate and authoritative information solutions to Chinese professionals in legal, tax and accounting, finance and healthcare fields.

Wolters Kluwer employs nearly 19,000 people worldwide with the revenue reached 4.61 billion euros in 2019. It is headquartered in Alphen aan den Rijn, the Netherlands and has offices in Europe, North America, Asia Pacific and Latin America to support clients’ needs globally. Wolters Kluwer shares are listed on NYSE Euronext Amsterdam (symbol: WKL) and are included in the AEX and Euronext 100 indices.