DATA PROTECTION LAWS OF THE WORLD

Netherlands vs China

DLA PIPER

NETHERLANDS

Last modified 18 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour* " (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Dutch GDPR Implementation Act (*Uitvoeringswet AVG*, the **Implementation Act**) constitutes the local implementation of the GDPR in the Netherlands. The Implementation Act follows a policy-neutral approach, meaning

CHINA

Last modified 18 December 2023

LAW

There is not a single comprehensive data protection law in the People's Republic of China (PRC). Instead, rules relating to personal information protection and data security are part of a complex framework and are found across various laws and regulations. That said, the three main pillars of the personal information protection framework in the PRC are the Personal Information Protection Law (PIPL), the Cybersecurity Law (CSL), and the Data Security Law (DSL).

On June 1, 2017, the CSL came into effect and became the first national–level law to address cybersecurity and data privacy protection. Draft Amendments to the CSL were issued on September 12, 2022, proposing enhanced liabilities for violating obligations of general network operation security, security protection of critical information infrastructure, network information security and personal information protection, etc.

The DSL came into force on September 1, 2021, and focuses on data security across a broad category of data (not just personal information).

Most significantly, the PIPL came into effect on November 1, 2021. The PIPL is the first comprehensive, national–level personal information protection law in the PRC. The PIPL does not replace — but instead enhances and clarifies — earlier personal information laws and regulations.

In addition to the PIPL, CSL and DSL, the following form the backbone of general personal information protection framework currently in the PRC:

- The Decision on Strengthening Online Information Protection, effective from December 28, 2012 (Decision);
- The Draft Regulation of Network Data Security Management, published for consultation on November 14, 2021;

that the requirements of the previous Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) are maintained insofar as possible under the GDPR. The Implementation Act provides for, among other things, national rules where this is necessary for the implementation of GDPR provisions on the position of the regulatory authority or the fulfilment of discretionary powers provided by the GDPR. There is a pending legislative proposal, the Data Protection Collection Act (*Verzamelwet gegevensbescherming*), that will affect the Implementation Act on a few specific topics. For example, adjustments will be made to the definition of criminal data and the existing derogations under the Implementation Act for the processing of biometric data will be further conditioned.

- The Measures for the Security Assessment of Outbound Data Transfers, effective from September 1, 2022; and
- The Measures for the Standard Contract for the Outbound Transfer of Personal Information, effective from 1 June 2023.

In the past five years, there has also been an abundance of implementing regulations and guidelines (herein referred to as Guidelines) proposed, issued or revised to flesh out the essentials and concepts introduced under the personal information protection framework. These include, non–exhaustively:

- National Standard of Information Security Technology — Personal Information Security Specification (PIS Specification), as amended and effective from October 1, 2020;
- Guidelines on Internet Personal Information Security Protection, effective from April 19, 2019;
- National Standard of Information Security Technology — Guidelines on Personal Information Security Impact Assessment, effective from June 1, 2021;
- Guidelines on Application of Security Assessment of Cross-border Data Transfers (First Version), effective from 1 September, 2022;
- Draft National Standard of Information Security Technology — Requirements for Classification and Grading of Network Data, published for consultation on September 14, 2022;
- Practicing Guidelines for Network Security Standards — Technical Specification for Certification of Personal Information Cross-border Processing Activities (V2.0), effective from December 16, 2022;
- Guidelines on the Filing of Standard Contracts for the Outbound Transfer of Personal Information (First Edition), effective from 1 June 2023; and
- Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong–Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong), effective from 10 December 2023.

The Decision has the same legal effect as law, and its purpose is to protect online information security, safeguard the lawful rights and interests of citizens, legal entities or other organizations, and ensure national security and public interests. While the PIS Specification and other Guidelines are only technical guides (covering in detail key issues such as data transfers, sensitive personal information and data subject rights), and thus

not legally binding, they have historically been highly persuasive. Although the PIPL takes precedence over the PIS Specification and other Guidelines, the PIS Specification and the Guidelines are still useful for the purposes of supplementing legislation, especially on any part that has not been addressed by the PIPL, CSL or DSL.

In addition to all of the above:

- provisions found in laws such as the Tort Liability Law have generally been used to interpret data protection rights *as a right of reputation* or *right of privacy*. However, such interpretation is not explicit. The PRC Civil Code, effective on January 1, 2021 further reinforces the statutory right of privacy for individuals and establishes data protection principles; and
- provisions contained in other laws and regulations may also apply depending on the industry or type of information involved (for example, personal information obtained by financial institutions and e-commerce businesses, personal information collected by telecom or Internet service / content providers, healthcare and genetic information, etc.). Applicability of other laws or regulations (including provincial level laws), such as the PRC Criminal Law, PRC E-Commerce Law, PRC Consumer Rights Protection Law and the new local data laws at a provincial level will invariably depend on the factual context of each case and further independent analysis is recommended.

Given the personal information protection framework is still evolving, and further regulations accompanying the new PIPL and DSL are anticipated to be published in the coming months, it is recommended that organizations continue to monitor the developments of the PRC data protection regulatory framework.

Extra-territorial scope

The PIPL has extra–territorial effect, and applies both to:

- data processing activities within the PRC; and
- processing of PRC residents’ data outside of PRC where:
    - for the purposes of providing products or services to PRC residents;
    - for analytics or evaluation of behavior of PRC residents; or
    - for any other reasons as required by law or regulations.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions are largely the same as in Article 4, GDPR. In addition, the Implementation Act defines "personal data concerning criminal law matters" as personal data concerning criminal convictions and offences or related security measures as referred to in Article 10, GDPR, as

The PIPL applies to both the public and private sectors.

DEFINITIONS

Definition of personal data

The PIPL defines personal information as any kind of information relating to an identified or identifiable natural person, either electronically or otherwise recorded, but excluding information that has been anonymized.

Definition of sensitive personal data

The PIPL defines sensitive personal information as information that, once leaked or illegally used, will easily lead to infringement of human dignity or harm to the personal or property safety of a natural person, including (but not limited to): (i) biometric data; (ii) religion; (iii) specific social status; (iv) medical health information; (v) financial accounts; (vi) tracking / location information; and (vii) minors’ data.

well as personal data relating to a prohibition imposed by the courts for unlawful or objectionable conduct.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the DPC in Ireland). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) has been appointed by law as the supervisory data protection authority and supervises compliance with the GDPR and the Implementation Act.

The Dutch Data Protection Authority's contact details are as follows:

NATIONAL DATA PROTECTION AUTHORITY

The PIPL has now clarified that the Cyberspace Administration of China (CAC) is primarily responsible for the overall planning and coordination of personal information protection and related supervision. Prior to the PIPL coming into force, various other legislative and administrative authorities have also claimed jurisdiction over data protection matters, and may continue to play some form of role in the context of personal information protection, such as:

- National People's Congress Standing Committee Ministry of Public Security;
- Ministry of Industry and Information Technology State Administration for Market Regulation; and
- Ministry of Science and Technology.

It is also anticipated that the local Public Security Bureau branches and industry regulators will still have a role in both management and enforcement of data protection; and the TC260 technical committee will continue to have delegated responsibility to publish technical standards.

Notwithstanding the CAC’s newly-clarified role, sector-specific regulators, such as the People's Bank of China or the China Banking and Insurance Regulatory Commission, may also monitor and enforce data protection issues of regulated institutions within their sector.

Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ DEN HAAG

Telephone number

(+31) - (0)70 - 888 85 00

Website

autoriteitpersoonsgegevens.nl

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale

REGISTRATION

Generally, there is no legal requirement in the PRC for data users to register with the data protection authority.

That said, there are specific registration requirements imposed on the sharing and transferring of specific categories of data (e.g. human genetic resources), and proposed filling requirements for security impact assessments (see Cross Border Transfers).

DATA PROTECTION OFFICERS

Under the PIPL, organisations which meet certain data processing volume thresholds (as yet unspecified by the CAC) are required to appoint a Data Protection Officer (DPO), and to register the name(s) and contact details of the responsible person with the relevant data protection authority.

For organisations based outside of the PRC, but processing PRC personal information, a specific representative or organisation within the PRC should be

- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection laws and practices, though it is possible to outsource the DPO role to a service provider (Article 37 (6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Implementation Act (Article 39) provides more detailed information regarding the secrecy requirement set out in Article 38(5) GDPR, by stipulating that the DPO must maintain the secrecy of any information that becomes known to him or her pursuant to a complaint by or request from a data subject, unless the data subject agrees to disclosure.

appointed, and details reported to the data protection authority.

Details of how and when the DPO or representative (as the case may be) should be registered is awaited.

Whilst the authorities have yet to announce the volume threshold for DPO requirements applicable under the PIPL, the PIS Specification requires an organization to appoint a data protection officer and a data protection department if the organization:

- has more than 200 employees and its main business line involves data processing;
- processes personal information of more than 1,000,000 individuals, or is estimated to process personal information of more than 1,000,000 individuals; or
- processes sensitive personal information of more than 100,000 individuals.

Organisations must register their DPO with the Dutch Data Protection Authority *(Autoriteit Persoonsgegevens)*. The registration form is available here.

A special email address and phone number is available for registered DPOs to contact the Dutch Data Protection Authority in case of questions with regard to the tasks of DPOs and GDPR compliance.

The contact details are as follows:

Email address: FG@autoriteitpersoonsgegevens.nl

Phone number: (+31) (0)70-8888660

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with

COLLECTION & PROCESSING

Collection

Consent

In general, express, informed consent is required from the data subject before personal information can be collected, used, transferred or otherwise processed. In certain circumstances, such as collecting or processing sensitive personal information, overseas data transfers and direct marketing, separate consent (i.e. explicit consent specific to the processing activity / transfer (rather than just general consent to the privacy notice, expressed through an affirmative action) is required from the data subject. Collection from individuals under 14 years old is prohibited unless explicit consent is obtained from their legal guardians.

In addition, the PIPL requires separate consent to be obtained for:

- processing sensitive personal information;
- overseas transfers;
- public disclosure of personal information;
- to provide data to another data controller for processing; and
- use of image or identification data collected in public through image or identification device for purposes other than maintaining public security.

Whilst there is no clear definition of what “ separate consent” constitutes in practice, it appears to suggest that organisations should avoid bundled or forced consent.

the GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject

The PIPL also introduced limited circumstances (i.e. lawful bases) in which personal information can be processed without consent, including:

- entering into or fulfilling a contract where the data subject is a named party;
- carrying out human resources management under an employment policy legally established or a collective contract legally concluded;
- fulfilling legal obligations (which may be helpful in the context of regulatory investigations);
- protecting the interests of natural person during any public health emergency or otherwise responding to a public health emergency, or in an emergency to protect the safety of natural persons’ health and property;
- carrying out news reporting and public opinion monitoring for public interests;
- the personal information being processed is already made public legally and the processing is within the reasonable scope and in accordance with the requirements of the PIPL; and
- as required by law (e.g. where required to disclose information under another PRC law).

However, in practice, it is unclear how these lawful bases could be relied upon. Consent remains the primary basis for lawful data processing, and it is anticipated this will continue in practice.

Notice

In addition to obtaining consent, a data controller (i.e. the organization who has the authority to determine the purposes, means or method of processing) should provide data subjects with a privacy policy or other form of notice, informing them of the scope and ways in which their personal information is collected, processed and disclosed, including the following information:

- the identity of the data controller, including its registered name, registered address, principal office, a telephone number and / or an e-mail address;
- a list of personal information collected for each business purpose. Where sensitive personal information is involved, relevant consent shall be explicitly marked or highlighted;
- the location of storage, retention period, means of use / processing and scope of the personal information collected; the purposes sought by the data controller, i.e. what the data controller uses the data for (for instance, supplying goods and

- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at

services, creating a user account, processing payments, managing subscriptions to the newsletters, etc.). These should be as comprehensive as possible, as additional purposes will require new consent;
- circumstances under which the data controller will transfer, share, assign personal information to third party processors (including intra-group entities) or publicly disclose personal information, the types of personal information involved in these circumstances, the types of third party data recipients, and the respective security and legal responsibilities of the entities;
- circumstances under which the data controller will transfer, share or assign personal information to third party controllers, the names and contact information of third party controllers, purpose and means of processing and personal information categories;
- circumstances under which the personal information will be transferred, accessed or stored outside of the PRC, the names and contact information of overseas recipi-ents, purpose and means of processing, personal information categories and the means and procedures for individuals to exercise their data subject rights against the overseas recipients;
- the rights of data subjects and mechanisms for them to exercise such rights, e.g. methods to access, rectify or delete their personal information, to de-register their accounts, withdraw their consent, obtain copies of their personal information and restrict automated decision by the data system etc.;
- potential risks for providing personal information, as well as possible consequences for not providing the data; data security capabilities of, and data security protection measures to be adopted by, the data controller and, when necessary, the compliance certificates related to data security and personal information protection; and
- channels and procedures for making inquiries and lodging complaints by data subjects, as well as external dispute settlement body and contact information.

The information in the privacy policy must be true, accurate and complete. The contents of the privacy policy must be clear and easy to understand, and ambiguous language should be avoided. The privacy policy should be made available to the data subject when collecting consent, and published publicly and easily accessible, for

the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12 (1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing

example, through a link placed prominently on a webpage or an installation page of a mobile application. When changes occur to the information provided in the privacy policy, the data subjects should be notified of such changes and (depending on the extent of changes made) further consent may need to be obtained.

Processing

Collection and processing of personal information must be directly related to the purpose of processing specified in the privacy notice.

Excessive data collection must be avoided. Interestingly the provisions of the PIPL around data minimization appear to be targeted at apps and big data analytics. On March 1, 2022, the Administrative Provisions on Recommendation Algorithms in Internet-based Information Services came into effect, which require recommendation algorithm-based service providers to establish management systems and technical measures for data security and personal information protection.

Additional restrictions are placed on use of biometric data collected in public places.

There are prohibitions on illegal collection, use, processing, sale, disclosure and transfer of personal information.

Impact assessment and record-keeping

The PIPL requires data controllers to undertake personal information impact assessments (PIIA) and to retain the results and processing records (for three years) in the following circumstances:

- processing of sensitive personal information;
- using personal information to conduct automated decision-making;
- appointing a data processor;
- providing personal information to any third party (likely to include sharing with group companies);
- public disclosure of personal information;
- overseas transfer of personal information; and
- any other processing activities that may have "significant impact to an individual".

A PIIA should include an assessment on:

- whether the purpose of use and means of processing is legitimate, proper and necessary;
- impacts and risks to individual’s interests; and

- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

- applicability of protection measures and risk appetite.

The “Guidance for Personal Information Security Impact Assessment” (PIIA Guidelines) (published by the National Standardization Technical Committee for Information Security) came into force on June 1, 2021.

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “ compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision taking, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (i.e. opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Special categories of personal data (Article 9)

Article 9(2) of the GDPR provides for a number of exceptions under which special categories of personal data may lawfully be processed. Certain of these exceptions require a basis in Member State law.

Division 3.1 of the Implementation Act provides for various exceptions for the processing of different types of special categories of personal data, subject to stringent conditions. Important examples include exceptions for:

- Scientific or historical research or statistical purposes
- The processing of personal data revealing racial or ethnic origin
- The processing of personal data revealing political opinions for the performance of public duties
- The processing of personal data revealing religious or philosophical beliefs for spiritual care
- Genetic, biometric and health data

Criminal convictions and offences data (Article 10)

The processing of criminal conviction or offences data is prohibited by Article 10 of

the GDPR, except where specifically authorized under relevant Member State law.

Division 3.2 of the Implementation Act provides several exceptions for the processing of criminal convictions and offences data.

The following general grounds for exemptions for processing criminal convictions and offences data apply:

- Explicit consent by the data subject
- Protection of a data subject's vital interests
- Processing related to personal data manifestly made public by the data subject
- Processing necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity
- Processing necessary for reasons of substantial public interest
- Processing necessary for scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) of the GDPR, and the conditions referred to in Section 24(b) to (d) of the Implementation Act have been met

Specific exceptions may apply on the basis of Article 33 of the Implementation Act, *eg,* where the processing is carried out by bodies that are responsible pursuant to law for applying criminal law, or where the processing is necessary in order to assess a request from the data subject to take a decision on him or her or to provide a service to him or her.

Child's consent to information society services (Article 8)

The Netherlands did not make use of the option to provide for a lower age limit for the processing of personal data of a child on the basis of Article 8, GDPR.

Automated Decision Making (Article 22)

The Netherlands has made use of the possibility provided by Article 22(2)(b) GDPR, and has implemented exceptions from the prohibition on

automated individual decision-making. Article 40 of the Implementation Act sets out that Article 22 (1) of the GDPR does not apply if the automated individual decision-making, other than based on profiling, is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out for reasons of public interest. Examples provided by the Explanatory Memorandum to the Implementation Act concern situations where there may be automated individual decision making on the basis of strictly individual characteristics, *eg,* in the case of awarding certain allowances (*eg,* study allowances, child allowances), where there is no reason to require human intervention. In such cases, the controller must take suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. Such suitable measures will in any case have been taken if the right to obtain human intervention, the data subject’s right to express his or her point of view and the right to contest the decision, have been safeguarded.

Processing of national identification number (Article 87)

Article 87 of the GDPR sets out that Member States may further determine the specific conditions for the processing of a national identification number. The Netherlands has made use of this possibility: Article 46 of the Implementation Act sets out that a national identification number may only be processed where explicitly allowed by law, and only for those purposes stipulated by the relevant law.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy

TRANSFER

If a data controller wishes to share, disclose or otherwise transfer an individual's personal information to a third party (including group companies), the data controller must:

- if the third party is a separate data controller, inform the data subject of the purposes of the sharing, disclosure or transfer of the personal information the types of data shared, the name

decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework), Uruguay, Republic of Korea and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained;
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. The transfer is necessary for important reasons of public interest;
e. The transfer is necessary for the establishment, exercise or defence of legal claims;
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained;
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are

and contact information of the recipient, and obtain prior separate consent from the data subject;
- perform a personal information impact assessment (PIIA), and take effective measures to protect the data subjects according to the assessment results (e.g. putting in place a data transfer agreement or similar contractual protections) (see Collection & Processing);
- record accurately and keep the information in relation to the sharing, disclosure or transfer of the personal information, including the date, scale, purpose and basic information of the data recipient of the sharing or assigning;
- ensure personal information is only transferred where required for processing purposes; not share or transfer any personal biometric information or other types of particularly sensitive personal information where prohibited under relevant laws or regulations; and
- ensure contractual measures are entered into to require the data processor to comply or assist the data controller in complying with obligations under data protection laws.

Cross-border transfers

Most personal information can be transferred or accessed outside of the PRC providing the following compliance steps are taken:

- the data controller has completed one of the following mechanisms to legitimize overseas data transfer — for details please see below:
  - the organisation has passed a CAC security assessment;
  - the organisation has obtained certification from a CAC-accredited agency;
  - the organisation has put in place CAC standard contractual clauses (SCCs) with the data recipient and filed the signed SCCs with the local CAC together with a cross-border transfer specific PIIA report; or
  - for compliance with laws and regulations or other requirements imposed by the CAC;
- the data controller has adopted necessary measures to ensure the data recipient’s data processing activities comply with standards comparable to those set out in the PIPL. In practice this means initial due diligence, sufficient

only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State. A transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

After the European Court of Justice Decision of 16 July 2020 (Schrems II), international data transfers to countries that don’t have an equivalent level of protection can take place, if such transfers are based on the 2021 EU Standard Contractual Clauses (SCC). In addition, such in compliance with EDPB guidance, a transfer impact assessment must be conducted in order to assess whether there are reasons to believe that the laws and practices in the third country of destination prevent the recipient from fulfilling its obligations under the SCC.

For more information, please visit our Transfer - global data transfer methodology website.

contractual protections and ongoing monitoring etc.;
- notice and separate, explicit consent has been given / obtained (see above) from the data subject (see Collection &Processing); and
- a PIIA has been conducted (see Collection & Processing).

In terms of the mechanisms to legitimise overseas data transfer referred to above:

1. CAC security assessment

According to the Measures for the Security Assessment of Cross–border Data Transfers, a CAC security assessment is required for data controllers who meet any of the following thresholds:

- an organisation intends to transfer any “ important data” overseas;
- a CIIO intends to transfer any personal information overseas;
- a data controller which processes personal information of more than 1,000,000 individuals and intends to transfer personal information overseas; or
- a data controller who in aggregate transfers overseas personal information of more than 100,000 individuals, or sensitive personal information of more than 10,000 individuals since 1 January of the preceding year.

The CAC security assessment involves the organisation completing a self–assessment of its cross-border data transfers, which must then be submitted for approval by both the local and national CAC. It primarily assesses the impact of overseas transfers on national security, public interest, and the legitimate rights and interests of individuals or organisations. If the CAC security assessment is passed, the organisation will be granted with a written approval. Such approval should be renewed every two years, or updated if there are changes to the cross–border transfers.

For organisations that must follow the CAC security assessment route, a copy of the data must in practice be stored locally in the PRC.

2. China SCCs

For PRC data controllers that do not meet the threshold for the CAC security assessment, they must put in place the China SCCs with the overseas data recipient, and then within 10 working days after the effectiveness of the

China SCCs file a copy of the signed SCCs with the local CAC branch together with the corresponding PIIA.

The Measures for the Standard Contract for the Outbound Transfer of Personal Information and the Guidelines on the Filing of Standard Contracts for the Outbound Transfer of Personal Information provide clarification on how the SCCs may be implemented by organisations as one of the mechanisms for overseas data transfer under the PIPL, how to prepare the corresponding PIIA by using the standard template formulated by the CAC and the procedures for filing the signed SCCs and the PIIA report.

3. CAC certification

The CAC certification route applies to organisations not caught by the CAC security assessment or SCCs route, and appears largely in practice to catch non-PRC data controllers who do not meet the CAC security assessment threshold. According to the Practicing Guidelines for Network Security Standards — Technical Specification for Certification of Personal Information Cross–border Processing Activities (V2.0), it will once implemented set up a framework of certification of overseas data transfer, including the principles, data protection obligations of data controllers and the overseas recipient, ensuring data subject rights, etc. Details to implement the certification remain unclear.

Organisations within regulated industry sectors may have to follow other compliance steps prescribed by their industry regulator to transfer or remote access their personal information outside of the PRC.

However, certain personal information (and non– personal data) must still remain in (and cannot be accessed outside of) the PRC. This includes (this is not an exhaustive list):

- certain data under industry–specific regulations (such as in the financial services sector and genetic health data); and
- certain restricted data categories (such as “state secrets”, some “ important data”, geolocation and online mapping data etc.).

The Draft Network Data Security Management Regulation also proposes introducing annual data overseas transfer security report to the CAC as well as other record keeping requirements.

Finally, according to the PIPL:

- a new publicly–available entity list may be published, listings foreign organisations to whom local PRC organisations may not transfer personal information, where such transfer may harm national security or public interest; data controllers must not provide personal information stored within the PRC to overseas legal or enforcement authorities unless approval is obtained from a designated Chinese authority. It remains unclear whether this extends to, say, requests from overseas industry regulators; and
- the PIPL clarifies that Chinese authorities may provide personal information stored within the PRC to overseas legal or enforcement authorities upon request, if and to the extent that there are international treaties or regulations in place to maintain fairness and for mutual benefit.

4. Transfer of personal information within the Greater Bay Area

Given the close integration of cities within the Guangdong–Hong Kong–Macao Greater Bay Area (GBA), and that data flows between Hong Kong and other cities within the GBA are becoming increasingly frequent, the CAC and the Innovation, Technology and Industry Bureau of the Government of the Hong Kong Special Administrative Region (ITIB) and Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) together formulated the Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong– Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong) (GBA SCCs).

In addition to complying with other general data protection requirements (e.g. notice, consent and impact assessment, etc.) if the data controller and the data recipient are registered in Guangzhou, Shenzhen, Zhuhai, Foshan, Huizhou, Dongguan, Zhongshan, Jiangmen, Zhaoqing or Hong Kong SAR, they may consider signing the GBA SCCs to legitimize the transfer and file the signed GBA SCCs with the Guangdong CAC and PCPD.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the

SECURITY

According to the CSL, DSL and PIPL, organizations must keep personal information confidential and establish a data security management system. This includes taking appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction of, or damage to, personal information. The measures taken must ensure a level of security appropriate to the harm that may result from

risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

An important security measure in line with the GDPR applicable from 1 January 2021 is that, most online payments must be completed with two-step verification. This is an obligation under the Payment Service Directive 2, the European directive for payments by consumers and businesses.

The Netherlands have not implemented any specific regulations on the basis of Articles 24, 25 or 32 of the GDPR. In this respect, the Explanatory Memorandum to the Dutch Implementation Act explains that no general standard will be developed which sets out when an organization has fulfilled its technical and organizational security obligations. However, specific sectoral codes of conduct may be implemented which may contain further concrete standards. For example, in the health sector we see that such security standards already exist (e.g. NEN 7510, which applies as an important information security standard in the health sector).

such unauthorized or unlawful processing, accidental loss, destruction or damage, and appropriate to the nature of the data. Security measures must be deployed, as prescribed by the CSL and DSL and their underlying measures, guidelines and technical standards (including the TC260 guidelines). The PIPL includes a specific obligation on data controllers to adopt corresponding encryption or deidentification technologies, and to adopt access controls and training.

Systems should also be established to handle complaints or reports about personal information security, publish the means for individuals to make such complaints or reports, and promptly handle any such complaints or reports received. Organizations must conduct mandatory data / cyber security training.

Additional security safeguards must be applied to processing of sensitive personal information and organizations deemed CIIOs (see above).

The CSL implemented a multi-level protection scheme for cybersecurity protection of information systems by network operators. Information systems are classified into 5 tiers and the security standard goes higher from tier 1 to tier 5. Organizations should conduct a self-evaluation and determine the tier(s) to which its information systems belong, based on relevant laws, regulations and guidelines. Filing to the Public Security Bureau is required and, in certain circumstances, assessment by accredited third party may also be required, depending on the determined tier level of a respective information system. Further national standards and guidelines have been published to provide further details and requirements on the process and technical aspect of the tiered system.

The DSL proposes introducing a similar tiered-security scheme for classification of data in due course (details have not yet been published).

Industrial regulators in each sector are working on issuing the data classification scheme in the relevant sectors. In particular, the Ministry of Industry and Information Technology recently issued the Measures for Data Security Management in the Industrial and Information Technology Sector (for Trial Implementation) (MIIT Measures) which came into force on January 1, 2023. The MIIT Measures provide standards for data classification and grading scheme in the industrial and information technology sector and classify data into three grades: general data, important data, and core data. Additionally, the Draft National Standard of Information Security Technology — Requirements for Classification and

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The provisions regarding data breach notifications are mostly identical to Articles 33 and 34 GDPR.

Grading of Network Data provides the principles and methods for data classification and grading.

If a data controller appoints a data processor to process personal information on its behalf, the data controller should ensure sufficient measures are adopted by the data processor to protect the personal information: for example, to conduct due diligence and regular audits on data processor to ensure the data processor adopts sufficient and adequate security measures; and put in place an appropriate data processing agreement with the data processor.

BREACH NOTIFICATION

Breach notification requirements are contained in the CSL, DSL and PIPL, and should be read together. “Network security incidents” that are notifiable are defined by reference to seven categories of different incident types, in particular:

1. Malicious program incidents;
2. Network attack incidents;
3. Data security incidents;
4. Information content security incidents;
5. Equipment and facility failure incidents;
6. Operational violation incidents;
7. Security risk incidents;
8. Abnormal behavior incidents;
9. Force majeure incidents; and
10. Other cyber incidents.

Guidelines set out other factors that should be considered whether a network security incident is potentially reportable. The China National Internet Emergency Center may be contacted in case of doubt as to whether an incident is potentially reportable.

An incident must be immediately notified: (i) internally, to the DPO; and (ii) externally, to the regulator (the PIPL refers to the CAC establishing (local) “personal information protection departments” (PIPD) for such purposes, but this is yet to be confirmed), and should include:

- affected data categories;
- reasons for the incident, and potential consequences;
- remedial measures, and mechanisms required by data controller to minimize impact; and
- contact information for data controller.

If the data controller can effectively avoid the disclosure, loss or tampering of data, the PIPL suggests that there is

Data breaches that require notification, should be notified to the Dutch DPA by completing an online form through the Dutch DPA website.

The form is available here.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital

no need to notify data subjects. Otherwise (and as per the CSL and DSL) data subjects must be notified immediately if the actual or suspected network security incident may result in harm to the rights and interest of the affected data subjects. Further, if the PIPD believes it may cause impact to individuals, they may request that the data controller notifies individuals. Similar information must be given to the data subjects alongside advice on how to protect against risks arising from the incident.

Further changes are also expected in this regard. Notably, the Draft Network Data Security Management Regulation (intended to supplement the PIPL) clarifies that incidents involving any of the following must be notified to the CAC and other relevant regulators within eight hours of the data incident:

- personal information of more than 100,000 individuals; or
- any important data.

A second report to the CAC is then required within five working days of the incident being resolved.

In any case, immediate remedial action must be taken in the event of any suspected or actual data disclosure, loss or tampering.

Organizations should also adopt proactive measures to minimize the risk of personal information breaches or security incidents, including but not limited to, implementing and testing a data incident contingency plan and organizing training.

We understand the regulators are working on a project to publish further guidelines as to how network security incidents should be managed. On 8 December 2023, the CAC released the Draft Administrative Measures on Cybersecurity Incident Reporting to solicit public opinions. This draft proposes new mechanisms to classify cybersecurity incidents and new reporting obligations.

ENFORCEMENT

Possible enforcement of, and sanctions for, a data protection breach in the PRC will depend on the specific data protection laws and regulations breached. Sanctions in relation to data protection breaches are scattered across various different laws and regulations, and the measures described below may not be comprehensive in all situations, as additional laws or regulations may be applicable depending on the industry or type of information at hand.

150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of undertaking. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects’ rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Taking the PIPL by way of example, it provides a range of sanctions, including (*inter alia*):

- enforcement notices and warnings;
- administrative fines of up to (for the most serious offences) 5% of the previous year’s annual revenue (unclear if local or
- global revenue) or up to RMB million, and confiscation of unlawful income. Note the PIPL imposes much higher fines than
- under other existing data privacy regulations);
- cessation of processing;
- suspension of apps and / or services;
- suspension of business;
- suspension of management / officials role;
- criminal sanctions (for certain offences, and under relevant criminal laws);
- civil claims; and
- social credit score or equivalent business credit files may be affected.

While the PIPL has now introduced higher fines, we anticipate that in practice the operational and contractual risks faced by organisations not complying with the PRC’s data privacy framework — alongside increasing reputational risks — remain very significant and should be managed very carefully.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered material or non-material damage as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of non-material damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

On the basis of Article 58(6) GDPR and in addition to the power to impose fines pursuant to the GDPR, the Dutch DPA has the power to impose an administrative enforcement order (*last onder bestuursdwang*) or an order subject to penalty (*last onder dwangsom*) to enforce obligations laid down by or pursuant to the Implementation Act.

ELECTRONIC MARKETING

The GDPR applies to most electronic marketing activities, as these will involve some use of personal data (e.g. an

ELECTRONIC MARKETING

Direct marketing by electronic means is only possible if the targeted consumers have explicitly consented to

email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted.

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Dutch legislation

Electronic marketing is partially regulated in Article 11.7 of the Dutch Telecommunications Act (Tw). The first paragraph of Article 11.7 of the Tw is the rules for telemarketing that does not involve human intervention. These so-called automatic systems for transmitting commercial, idealistic or charitable communications may only be used if the consumer has given his prior consent. As of 1 July 2021, the Dutch Telecommunications Act changed. As a main rule, also for telemarketing with human intervention, the opt-in system will be used.

New Legislation

The ePrivacy Regulation is a proposed regulation governing the use of electronic communication services within the European Union and is intended to replace the Directive on privacy and electronic communications (Directive 2002/58/EC). In addition to the GDPR, the ePrivacy Regulation represents a core element of EU-level data protection. On 10 February 2021, the Council of the European Union ('the Council') published a new legislative proposal, thereby launching negotiations between the Council, the European Parliament and the European Commission.

In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

ONLINE PRIVACY

Traffic Data

receiving such messages either at the time their electronic address / mobile phone number was collected or at a later time.

Specific information must be stated in each electronic message: for example, the identity of the entity sending the message, and a mark identifying "*Guang gao*" (which means advertisement in Chinese) or "AD" on a direct marketing message.

There are also specific rules applicable to direct marketing by text messages (SMS), and certain specific prescribed information must be provided to data subjects at the time their mobile phone number was collected or prior to sending direct marketing text messages.

ONLINE PRIVACY

Traffic Data is regulated in Article 11.5 of the Tw. Traffic Data held by a public electronic communications services provider (CSP) must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- It is being used to provide a value added service; and
- Consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CSP for:

- The management of billing or traffic
- Dealing with customer enquiries
- The prevention of fraud
- The provision of a value added service (subject to consent)
- Market research (subject to consent)

Location Data

(Traffic Data not included) – Location Data is regulated in Article 11.5a of the Tw. Location Data may only be processed:

- If such data is being processed in anonymous form; or
- With informed consent of the individual.

Cookie Compliance

The Netherlands implemented the E-Privacy Directive through the Dutch Telecommunications Act in Article 11.7a. The Authority for Consumers and Markets (ACM) is entrusted with the enforcement of Article 11.7a of the Tw. In addition, in relation to cookie compliance all privacy requirements from the GDPR must be taken into account. The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) has been appointed by law as the supervisory data protection authority and supervises compliance with the GDPR and the Dutch GDPR Implementation Act.

The main rule is that the website operator needs to obtain prior consent from a user before using cookies (opt-in) and needs to clearly and unambiguously inform the user about these cookies (purpose, type of cookie, etc.). Please note that the website operator is not entitled to refuse users access to its website(s) if no consent is given. The requirement to obtain prior consent from a user does not apply in case of functional cookies (e.g. to enable web shopping carts or language choices) and analytical cookies that have little or no impact on the

The general compliance obligations applicable to processing of personal information under the PIPL apply to the online (and offline) environments. In addition, the PIPL imposes additional compliance obligations on organisations that fall into one of the following categories:

- “important internet platform providers”;
- data controllers processing data of a “ large volume of users”; or
- “complex businesses”.

It is still unclear which organisations would fall within these categories, but these organisations must comply with additional measures when processing personal information, namely:

a. set up personal information protection compliance mechanisms;
b. set up external independent data protection organisations to supervise data protection mechanisms;
c. establish platform regulations;
d. establish and publish processing obligations and processing rules that regulate products and service providers in an open and fair manner;
e. stop the provision of products or service providers if they violate the law or regulations as regards processing of personal information; and
f. publish from time to time social responsibility reports as regards processing of personal information.

In terms of automated–decision making and profiling:

- analytics or evaluation based on computer programme around behavior, interests, hobbies, credit information, health or decision making activities, must be transparent, open and fair, and should not apply any differential treatment between individuals; and
- any push information or business marketing should not be directed to an individual’s character and should provide individuals with a convenient way to opt out.

As well as the PIPL, the CSL, Consumer Protection Law and E–Commerce Law offer protection to consumer / user personal information. As well as personal information protection, under these rules data controllers should strengthen management of information provided by users, prohibit the transmission of unlawful

user's privacy (e.g. for testing the effectiveness of certain banners / pages with the aim to improve the website). In such case, the website operator still needs to inform the website visitors about the cookies.

The information collected through cookies are considered personal data, unless the party that places the cookies can prove otherwise.

In case of violation of electronic marketing or online privacy legislation, the ACM can impose fines of up to EUR 900,000 per violation. In some cases, the fine may be even higher and amount to a percentage of the total annual turnover. In case of violation of the GDPR and the Dutch GDPR Implementation Act, the Dutch Data Protection Authority can impose fines up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

KEY CONTACTS

Richard van Schaik
Partner
T +31 20 541 9828
richard.vanschaik@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

information and take necessary measures to remove any infringing content, then report to supervisory authorities. Sufficient notice and adequate consent should be obtained from data subjects prior to the collection and use of personal information. Further obligations are imposed on mobile apps providers including but not limited to conducting real–name identification, undertaking information content review.

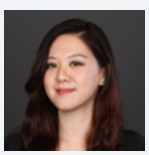
In recent years, the regulators have also issued a range of guidelines targeting mobile app providers. These guidelines introduce specific data protection and privacy obligations aiming to regulate the data collection practices and processing activities of mobile app providers. There has also been a crackdown against (suspected) non–compliant mobile apps. Organisations are advised to review their app compliance as a matter of priority.

Data subject rights (under the PIPL and other laws within the personal information framework), include rights to access and obtain information about their data held and processed, to correct their data, to request deletion of data in the event of a data breach, to object to automated decision–making and to de–register their account etc. Most importantly is the right to withdraw consent to personal information processing.

There are currently no specific requirements regarding cookies within existing laws or regulations in the PRC. However, the use of cookies and / or similar tracking technologies, to the extent they constitute processing of personal information, should be notified to data subjects as part of a privacy policy and adequate consent should be obtained from data subjects for such use.

KEY CONTACTS

Carolyn Bigg
Partner, Global Co-Chair of Data Protection, Privacy and Security Group
T +852 2103 0576
carolyn.bigg@dlapiper.com



Venus Cheung
Registered Foreign Lawyer
T +852 2103 0572
venus.cheung@dlapiper.com

Amanda Ge
Of Counsel
DLA Piper

T +86 185 1511 8230
amanda.ge@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.