The EU General Data Protection Regulation

The EU General Data Protection Regulation ('GDPR') is fast approaching. After a two-year implementation phase, the new Regulation will be coming into force on 25 May 2018. It is Europe's biggest shift in data protection law for the last decades. Not only European companies are affected. Based on the extra-territorial effect of the GDPR, numerous Hong Kong entities will face substantial challenges adapting to the new requirements. This article examines the key provisions of the new Regulation, highlights potential liability risks and draws a comparison with the Hong Kong data protection regime under the Personal Data (Privacy) Ordinance (Cap. 486) ('Ordinance').

1.Introduction

Until the new Regulation enters into force, the Data Protection Directive ('DPD') remains the governing law in the EU. The DPD left space for substantial variation of national data protection regulations and was faced by a significant increase in cross-border data flows. The goal of the European legislators was to form a harmonized data protection landscape, providing a strong and coherent data protection framework.

The new law comes in the shape of a regulation and is directly applicable in all member states. However, there remains room for certain national differences. The GDPR provides for mandatory member state rules on supervisory authorities, provisions for "other sanctions" and on the reconciliation of data protection law with the right to freedom of expression and information. Optional member state rules may be issued with regard to Data Protection Officers or specific employment law.

2. Scope of the Regulation

2.1 Extra-territorial reach

The GDPR applies to the processing of personal data by an establishment of a controller or a processor in the EU, regardless where the processing takes place. It also catches any processing of personal data of data subjects who are in the EU related to the offering of goods and services in the Union or monitoring the behaviour of data subjects in the EU. In order to determine, whether a foreign company is offering goods and services in the EU, the mere access to a website or e-mail is not sufficient. Decisive factors can be the use of language or general currency used in at least one member state with the possibility of ordering goods and services in that other language.

This extended reach is not an exclusive provision under the GDPR. In fact, many other data protection regulations such as the Ordinance have certain extra-territorial effect. However, due to the size of the European Market and the strict provisions of the GDPR, combined with high potential sanctions, many foreign companies are forced to adapt their data protection scheme.

2.2 Processing personal data

Personal data are defined under the GDPR in a technology neutral manner very similar to the definition given under the Ordinance. However, the explicit inclusion of location data, online identifiers (eg cookies) and genetic data may result in additional obligations for companies processing such data. Whereas the Ordinance generally only provides direct compliance obligations for controllers, the GDPR imposes these obligations on both controllers and processors. This is most likely going to affect the way supply and other commercial agreements are drafted in regard of the new European rules.

3. Main provisions

3.1 Basis of lawful processing

3.1.1 Overview

Requirements on data processing are set out under Art. 6 of the GDPR. Whereas, the six bases of lawful data processing are (i) consent, (ii) contract, (iii) legal obligations, (iv) vital interests, (v) public task and (vi) legitimate interests. Personal data may be processed only if at least one of these bases applies.

Under the base of contract, data can be processed, if it is necessary to comply with the processor's contractual obligations towards the data subject or in case of a request of the data subject prior to entering into a contract (eg data to provide a quotation for an insurance contract). Legal obligations may be imposed by legal provisions or by a court request, which must arise under EU law or the laws of a member state. Hence, in case of a non-EU legal provision or court order, processors may face difficulties and might need to rely on another basis on data processing. Vital interest primarily covers certain cases of emergency medical care. Legitimate interest is the broadest base to collect data without consent. However, a legitimate interest has to exist, it has to make processing necessary and in particular, the individual's interest and the processor's interest have to be balanced. In this regard, companies should keep record, to demonstrate that they made a legitimate interest assessment and observed the steps mentioned above. It should be noted, that also processing carried out on the basis of legitimate interest may be subject to objections from data subjects.

3.1.2 Consent

One of the key foundations of lawful data processing under the GDPR is the data subject's consent pursuant to Art. 7. The requirements in this regard have been increased, compared to the previous regulation under the DPD. However, pre-GDPR consent does not have to be automatically refreshed. It remains valid insofar as it is in line with the conditions laid down in the GDPR. Notably, the new law provides some important differences, eg relying on "presumed consent" will not be sufficient any more.

Consent does not have to be given in a particular form, but data processors have to be able to provide proof of their consent to data use. Consent may be withdrawn at any time. The data subject shall be informed about this option in advance and it shall be made easy to give such declaration. In particular, the data subject has to be able to withdraw in the same form, which was used obtaining consent (eg via a website, an app or by e-mail). Once consent has been given, the company should still check in appropriate intervals, if a "refreshment" is necessary.

Valid consent has to be (i) freely given, (ii) specific, (iii) informed and (iv) unambiguously indicated. Consent is only freely given, if the individual is unable to refuse or withdraw his or her consent without detriment. Due to the nature of the relationship between employer and employee, consent is unlikely to be considered "free" in this regard. In general, companies should pay particular attention to avoid any bundling the performance of a contract, including the provision of a service, with consent on data that is not necessary for the performance of that contract. Specific purpose for the data processing has to be determined, which avoids gradual widening or blurring of purposes (so called "function creep"). Being informed overall is a key requirement for valid consent. This includes information such as the controller's identity, the purpose and the type of data. Under the GDPR, consent requires a statement from the data subject or a clear affirmative act. Hence, consent must always be given through an active motion or declaration.

The GDPR provides stricter and more detailed rules for valid consent than the Ordinance. Hong Kong companies within the scope of the GDPR that rely on the consent of data subjects as a lawful basis for any of their processing activities should ensure that they meet the requirements highlighted above.

3.2 Principles relating to processing of personal data

Art. 5 (1) of the GDPR contains several principles of data processing. Data may only be processed in a lawful, fair and transparent manner. Under the principle of data minimisation, data processing has to be limited to what is necessary in relation to the purposes for which they are processed. The data must also be kept up to date and accurate. Moreover, the data must be processed in a manner that always ensures adequate security for the personal data.

Several provisions on accountability and governance support the enforcement of these general principles. The controller has to maintain extensive records of processing and shall make the records available to the supervisory authority upon request. A new feature is data protection by design and by default, which does not exist under Hong Kong law. By design means taking into account the potential data protection issues already throughout the process of designing a new product or service. Furthermore, technical and organisational measures for ensuring that, by default, only personal data, which are necessary for each specific purpose of the processing, are processed shall be implemented.

3.3 Data Protection Officer

Data controllers and data processors must designate a Data Protection Officer ('DPO') under the GDPR in three cases: (i) if processing is carried out by a public authority, (ii) if the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale or (iii) if their activities consist of processing on a large scale of special categories of data. Member states may provide a lower threshold in their national law. The EU's WP 29 recommends in its guidelines, that the DPO should be located in the EU and should report directly to the highest management level.

Under Hong Kong law, there is no legal requirement to appoint a DPO. A best practice guide issued by the Commissioner recommends designating a responsible person to oversee the data users' compliance with the Ordinance. However, there is no specific enforcement action or penalty if a company does not appoint a DPO.

3.4 Data breach notifications

Another key change is the requirement of data breach notifications. The controller shall document any personal data breaches and shall notify the supervisory authority in case of a personal data breach, which is not unlikely to result in a risk to the rights and freedoms of natural persons. The processor shall notify the controller, if he is becoming aware of such data breach. Furthermore, the controller shall notify the data subject of a data breach, if it is likely to result in a high risk to the rights and freedoms of natural persons. Certain exceptions are provided, if appropriate protection measures were implemented and were applied to the respective case.

The Ordinance does not contain a statutory requirement on data users to inform data subjects or authorities about data breaches. The Commissioner only recommends such notification.

3.5 Data transfer

Under the GDPR, a uniform level of data protection will be created within the EU, which simplifies data transfer between member states. Companies that plan to transfer personal data to third countries have to check on two levels whether this data transfer is permitted.

In a first step, a legal basis must apply to the data processing as such together with all relevant provisions of the GDPR. Any international transfer of personal data must also meet the requirements of the other conditions under the GDPR.

In a second step, companies must comply with one of the bases of lawful data transfer set out under Chapter V of the GDPR. One possibility is data transfer under an adequacy decisions by the EU Commission, which has not yet been issued for either Hong Kong or China. Alternatively, data may be transferred under appropriate safeguards, such as contractual clauses agreed authorised by the competent supervisory authority or binding corporate rules for inter-group transfers. If no other base is applicable, Art. 49 of the GDPR contains certain exceptions such as explicit consent or necessity for the performance of a contract.

Compared to the GDPR, Hong Kong provides for equivalent requirements in terms of data transfer, which are set out in the Commissioner's guidelines. Under both data protection regimes, the goal is to ensure the own protection standard also in regard of international data transfer. However, legal obligations on data transfer under Sec. 33 of the Ordinance have not been enforced yet.

3.6 Rights of individuals

The new Regulation strengthens the rights of individuals. These namely consist of the right of information, rights to access, rectification and erasure, right to restriction of processing, right of data portability, right to object and the right not to be subject to automated decision making (eg profiling).

Data subjects' rights under the GDPR are generally more extensive than under Hong Kong law. Organisations from Hong Kong processing European data or having an establishment in Europe, have to ensure to observe all individual rights under the GDPR and especially be able to provide data according to the rules of data access and data transfer.

4. Sanctions

4.1 Administrative fines

The GDPR provides for severe administrative fines up to EUR 20,000,000.- or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher in case of infringements of the Regulation. "Undertaking" will most likely be defined in accordance with EU court decisions on competition law, which provide a broad definition. Hence, in many cases worldwide group revenues will be taken into account when calculating fines.

Fines under the Ordinance can be imposed only up to an amount of HKD 1,000,000.- and are not directly revenue based.

4.2 Civil liability

Pursuant to Art. 82 of the GDPR, individuals may claim for compensation of both material and non-material damages as a result of an infringement of the Regulation. In addition, companies may be liable under contractual provisions or national tort liability. Civil liability also exists under Hong Kong law and similarly includes non-pecuniary loss. However, the GDPR provides stricter rules on burden of proof and a wider scope of liability, including data processors.

Companies may reduce the risk of liability by adoption of codes of conduct or certification mechanisms to avoid data infringements and demonstrate compliance. However, these measures are not sufficient for the purpose of exception from liability. In general, companies will have to keep detailed documentation on data proceedings and protective measures. The general principles of accountability and governance result in a shift of burden of proof to the company. In many cases, not the individual will have to proof a data infringement, but rather the processor or controller will have to demonstrate compliance with the data protection provisions.

4.3 Other penalties and investigative powers

Other penalties must be imposed in member state law. Germany, for example, implied additional criminal sanctions under the new Bundesdatenschutzgesetz.

Supervisory authorities have a wide range of powers from investigations up to temporary or definitive limitation including a ban on processing and the issuing of public warnings.

5. Conclusion

The GDPR provides an elaborated regulatory system as a result of several decades of data protection in Europe and a long lasting legislation process. It is an important step towards full data harmonization within the EU, despite the possibility of differing member state laws in certain restricted areas. Detailed requirements and heavy fines provide challenges for all affected organisations. Hong Kong companies will not be able to fully rely on existing protection measures set out in accordance with the Ordinance, which is largely based on the former European DPD. Both regulations ensure a certain level of data protection. But in several areas highlighted in this article, the European Regulation goes beyond the Hong Kong requirements. Companies adapting to the new challenges and implementing measures like data protection by design and access ability of data may also benefit from the new, more efficient data processing and accounting systems. The new Regulation will enter into force soon and companies should take immediate steps to ensure compliance. However, several member state rules in specific areas and case law on the new provisions have yet to be established.

Andreas Respondek

Respondek & Fan Pte Ltd

Jasmin Eberhard

Respondek & Fan Pte Ltd

Johannes Schmidt

Respondek & Fan Pte Ltd