KROMANN
REUMERT

HOW WILL THE NEW EUROPEAN DATA PROTECTION REFORM IMPACT CHINESE COMPANIES?

August 2017

Tina Brøgger Sørensen
Partner

Mobile: +45 61 20 35 33
Direct: +45 38 77 44 08
tib@kromannreumert.com

Jan Ussing
Partner

Mobile: +45 61 61 30 10
Direct: +45 38 77 44 25
jus@kromannreumert.com

Chen Chen Hu
Legal Consultant

Mobile: +45 61 55 21 56
Direct: +45 38 77 41 40
chu@kromannreumert.com

Anna Sofia Kærsgaard
Advokat

Mobile: +45 51 38 15 36
Direct: +45 38 77 46 83
ask@kromannreumert.com

Daiga Grunte-Sonne
Advokat

Mobile: +45 61 20 99 95
Direct: +45 38 77 41 18
dso@kromannreumert.com

How will the new European data protection reform impact Chinese companies?

The new EU General Data Protection Regulation (GDPR) that enters into force on 25 May 2018 will impact companies around the world, including Chinese companies.The new regime imposes extensive obligations on both data controllers and data processors, which will take time to implement and prepare for, and non-compliance can result in severe fines. Therefore, all companies should start preparing now. In this article, we will give you a short introduction to applicable data protection rules in the EU, including the basic principles and concepts, a summary of the highlights of the future GDPR, an outline of some of the implications for China, and our recommendations of what steps to take to prepare for the future GDPR.

The new EU General Data Protection Regulation (GDPR) will impact companies around the world, including Chinese companies. The GDPR will apply to any company that acts as a data controller or data processor and that targets or monitors individuals in the EU, irrespective of whether such company is based in the EU. Further, the GDPR heralds some of the most stringent data protection rules in the world with fines of up to 4 % of the annual worldwide turnover for any non-compliance and should therefore attract the attention of companies around the world, as it places any company targeting or monitoring individuals – e.g. consumers, users, natural persons acting professionally – in the EU at risk of incurring severe fines. Therefore, all companies should familiarize themselves with the new set of rules, or at least investigate whether they will become subject to the new regime. On the positive side, the harmonization of rules will make it easier for companies to use a one-size-fits-all solution for the whole of the European market.

The GDPR will not apply until 25 May 2018. However, the new regime imposes extensive obligations on both data controllers and data processors, which will take time to implement and prepare for – especially for non-EU companies becoming subject to EU data protection rules for the first time – and all companies should therefore start preparing now.

An overview of general EU data protection rules and the GDPR

The concepts of data protection are not new in Europe, but compliance with the data protection rules has not always been given much importance by companies and individuals. However, the explosive increase in use of personal data and a higher public focus and scrutiny by regulatory authorities now require more diligence and adherence to legal requirements. This section summarises some of the basic principles and concepts of already applicable EU data protection rules.

EU member states implemented local laws respectively on the basis of the current EU Directive 95/46 on the protection of personal data from 1995. These are requirements that your company must comply with already, if the company falls under the scope of the directive.

Here are some of the highlights of the current EU data protection rules and the future GDPR:

General EU data protection rules

Basic concepts of the EU data protection rules
The EU data protection rules apply to the processing of personal data, by automatic means, for instance, a computerised system or database; and to the processing by other (non-automated) means that form part of a relevant filing system. Although the current rules on processing of personal data are not harmonized between all EU member states, many of the below general concepts apply across all of the states.

Personal data and processing
'Personal data' include any information that directly or indirectly allows for the identification of a natural person, such as name, address, location data, online identifier, customer number and employee number. Encrypted data is also regarded as personal data, unless such data is effectively anonymized, e.g. the encryption key has been effectively destroyed and the identity of the individual in question cannot be re-established. This definition is very broad, so in case your company is e.g. selling goods to European customers or providing services to European consumers as end users, your company will in fact be handling personal data.

The concept of processing is very broad as well. It includes any operation or set of operations performed on a set of personal data, such as collection, registration, systemization, storage, adaption or alteration, use, disclosure, dissemination or otherwise making available, blocking, and/or linkage or pooling of data. Even the mere erasure or destruction of personal data is regarded as processing of personal data. Processing of personal data is subject to a number of principles on processing, including rules on lawfulness of processing.

Further, EU data protection rules operate with the concept 'sensitive data', covering all personal data concerning or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life. Such sensitive personal data is subject to more stringent data processing rules.

Data controller and data processor
A 'data controller' is a natural person, legal entity or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data. A 'data processor' means a natural person, legal entity or other body that processes personal data on behalf of the data controller.

Lawfulness of processing
Personal data about an individual ('data subject') may only be processed if certain requirements are met. For instance, processing of general (non-sensitive) personal data may take place if the data subject has unambiguously given his or her prior consent to the processing of the personal data, or in certain other specified situations, for example, if the processing is necessary for (i) the performance of a contract to which the data subject is party, (ii) compliance with a legal obligation to which the data controller is subject or (iii) the purposes of the legitimate interests pursued by the data controller or a third party, unless such interests are overridden by the interests of the data subject. The data subject's consent must be given freely and must be specific and informed.

Data processing agreements
If a data controller engages a data processor to process personal data on its behalf, a written data processing agreement must be in place between the data controller and the data processor. This requirement also applies to data processors that engage sub-contractors (e.g. sub-processors) and intra-group processing operations, where one entity engages another entity of the group in processing personal data for which it is a data controller (for example, in relation to centralized retention of and access to HR or customer data).

Basic principles for processing of personal data
The general EU data protection rules include a number of overall principles on good data protection practice, which must be complied with whenever personal data are being processed, including:

- *Lawfulness, fairness and transparency:* Personal data shall be processed fairly and lawfully;
- *Purpose limitation:* Personal data may only be collected for specified, explicit and lawful/legitimate purposes and may not be further processed in a way incompatible with those purposes;
- *Data minimisation:* The personal data must be adequate, relevant and not excessive in relation to the purposes for which the data are collected and further processed. If the purposes sought can be achieved by using anonymous or non-identifying information, then such information must be used instead of personal data (for example, in test environments);
- *Accuracy:* Personal data must be accurate and, where necessary, kept up to date;
- *Storage limitation:* Personal data may not be processed for longer than what is necessary for the purposes for which the personal data were collected or for which the data are further processed.

Any processing of personal data that does not comply with the above principles will be regarded as contrary to the applicable EU data protection rules.

The GDPR

Main purposes
The main purposes of the GDPR are to:
- bolster the fundamental rights and freedoms of citizens in the EU (including the right to privacy) in a digital age, where the scale of data sharing and collecting has increased dramatically; and
- facilitate business in the EU by harmonizing the data protection rules and thereby reducing legal uncertainties and compliance costs for businesses operating and/or targeting or monitoring data subjects in the EU.

The GDPR will be directly applicable in all EU member states without the need for implementation of national legislation.

Background of GDPR and link to official text
The GDPR was adopted by the European Parliament on 14 April 2016. The GDPR will replace the current Directive 95/46 EC on the protection of personal data from 1995 and associated regulation in each state. The GDPR entered into force on 24 May 2016, but will not apply until two years after its effect. That is to say, that all businesses need to comply with the GDPR by 25 May 2018.
The official text of the GDPR in English can be found here.

Although the purpose of the GDPR was to harmonize the data protection rules in the EU, it is important to note that the GDPR – on several areas – allows member states to maintain and/or establish national sector-specific laws and/or rules to further specify the rules of the GDPR. This means that businesses operating and/or targeting or monitoring data subjects in the EU still need to be aware of any special local legislation in the member state(s) that are relevant for their business operations.

Extended territorial reach
The GDPR will apply to both EU and non-EU companies, if they:

(i) offer services and/or goods to citizens in the EU (even if it is for free) and thereby come into possession of personal data on data subjects in the EU, or

(ii) monitor the behaviour of data subjects in the EU, for example by use of cookies or similar profiling techniques, thereby coming into possession of such citizens' personal data.

The question of 'offering services and/or goods' would be determined on a case-by-case basis, the mere fact, that individuals in the EU can access a website of a non-EU company (for instance, a Chinese company's website in Chinese) will not constitute 'offering of services and/or goods'. However, if the website uses a language or a currency generally used in one or more member states in the EU and offers individuals in the EU the possibility to order goods or services from the website, then such non-EU company will most likely fall under the scope of the GDPR, if it comes into possession of personal data of such consumers.

GDPR and Chinese companies
Chinese companies will become subject to the GDPR, if (i) they are based in the EU, (ii) they offer services and/or goods to data subjects in the EU and thereby come into possession of personal data on EU citizens, (iii) they monitor behaviour of data subjects in the EU, or (iv) public international law prescribes application of EU member state law.

The GDPR also applies if public international law prescribes application of EU member state law, but in practice, the occasion where member state law applies due to public international law is very rare.

One-stop-shop
The GDPR introduces a 'one-stop-shop' mechanism, under which companies as a general rule only need to deal with one supervisory authority. However, in order to enable individual citizens to have their cases dealt with locally, the GDPR ended up establishing a detailed regime with a lead supervisory authority working together with other concerned supervisory authorities in respect of cross-border operations. Further, each individual supervisory authority will be competent to handle, or at least be actively involved in, any complaints or infringements of the GDPR, which are purely local. How the 'one-stop-shop' mechanism will work in practise remains to be seen.

Sensitive data
The concept of sensitive data is broadened to also include genetic data, i.e. any data relating to the inherited or acquired genetic characteristics, revealing unique information about a person's physiology or health, and biometric data, e.g. fingerprints and facial images, which allow to confirm the unique identification of the person in question.

Rights of data subjects
As mentioned above, one of the main purposes of the GDPR is to strengthen the fundamental rights and freedoms of the data subjects.

These rights include:
- a right of access to each individuals' own data, including detailed information on how such data is being processed and to whom it has been disclosed;
- a right to rectification, whereby data subjects can request that any inaccurate data concerning him or her is rectified;
- a right to data portability, whereby a data subject can request to receive personal data concerning him or her, which he or she has provided to a data controller, in a commonly used or machine-readable format or that such data are transferred to another data controller;
- a right to be forgotten, whereby data subjects can require the erasure of their personal data without undue delay in certain, further specified situations;
- a right to object to processing, including if personal data is processed for direct marketing purposes; and
- a right not to be subject to automated individual decision making, including profiling.

In general, any communication to data subjects relating to the processing of their personal data must be concise, transparent and intelligible and must be presented in an easily accessible form, using clear and plain language, especially if the data subject in question is a child.

Consent to processing
Under the GDPR, the requirements to a data subject's consent to the processing of their personal data are more stringent than under the current rules. For example, the data controller must inform the data subject prior to giving a consent that he or she may withdraw such consent at any time and consents given in writing must be clearly dis-

tinguished from other matters, for example, other provisions in a contract. Further, the data controller must be able to demonstrate that a valid consent has been obtained from the data subject.

Data transfer to China under GDPR
Prior to any transfer to China, a company should ensure that such transfer is legal. Data flow from the EU to China is legal only if: (i) entering the standard contractual clauses; (ii) adopt binding corporate rules; (iii) localisation of data centre. Please also note that regarding the 'adequacy decision' from the European Commission – it cannot exclude the possibility in the coming future that 'adequacy decision' being a decision from the European Commission that certain specified sectors within China have ensured an adequate level of protection of the rights and freedoms of individuals (including the right to privacy and protection of personal data), whereby personal data can be transferred freely to such specified sectors within China.

The consent in relation to processing of sensitive data must be 'explicit', e.g. the data subject must actively accept the processing of his or her sensitive data.

International data transfers
The GDPR and the current EU data protection rules impose certain restrictions on transfers of personal data to countries outside of the EU. In this context, it is important to note that 'transfer' of data also includes the potential remote access from a country outside the EU to any personal data in the EU, even only momentarily, e.g. if an employee from a Chinese company obtains access to servers placed in Europe. As of the date of this article, China is not among the countries recognized by the European Commission as providing 'adequate level of protection', personal data may thus only be transferred to China on the basis of:

- entering into the European Commission's standard contractual clauses ('EU-controller to Non-EU/EEA-controller' or 'EU-controller to Non-EU/EEA-processor') with the recipient of the data, as the clauses will ensure sufficient safeguards as required by the regulations;

- adoption of binding corporate rules as means of legitimising intra-group international data transfers (i.e. data transfers between members within the same group of undertakings) which requires prior approval by the data protection authorities; or

- an approved code of conduct or certification mechanism with binding and enforceable commitments of the data controller or data processor to apply appropriate safeguards. For the time being, such mechanism is only in place with the U.S. (the EU-US Privacy Shield), but it is expected that these will be established in relation to specific sectors or jurisdictions going forward.

Alternatively, the data controller may choose to establish data centres in the EU to avoid any transfers to China or other third countries. However, in such case the data controller must be aware of the broad definition of 'transfer' in the current EU data protection rules and the GDPR. Hence, remote access from countries outside the EU to personal data in the EU – even momentarily, e.g. in connection with IT support or similar – is considered 'transfer of personal data', rendering it necessary to establish an adequate level of protection in accordance with the GDPR.

Where the third country, to which the personal data are to be transferred, does not ensure an adequate level of protection, a transfer may take place nonetheless pursuant to certain limited derogations laid down in the GDPR. Such derogations include instances, where the data subject has explicitly consented to the transfer, after having been informed of the possible risks of such transfer, due to the absence of an adequate level of protection of its personal data. However, it should be noted that these exceptions in general are interpreted very restrictively.

Separate responsibilities and liability of data processors
Under current EU data protection rules, data processors, e.g. service providers that process personal data on behalf of a data controller, cannot be held directly liable for any violation of the data protection rules, including any breaches of data security. One of the key changes in the GDPR is that the data processors will have direct obligations, so in cases where it has not complied with obligations of GDPR directed to processors or it has acted outside or contrary to lawful instructions of the controller, the data processor can be held liable for violations of the GDPR. The obligations of the data processor include keeping records of the processing activities, implementing appropriate technical and organizational measures, appointing a data protection officer, and the data processor is liable for any breach of its obligations under the GDPR, including assuming a joint liability with the data controller towards any data subject.

Penalties
The GDPR has a two-tiered sanction regime, which significantly raises the level of fines to violations of requirements. Violations of some provisions in the GDPR, which have been deemed most important by the lawmakers (for instance, violation of the provisions regarding international data transfers or the basic principles for processing of personal data), can lead to administrative fines of up to EUR 20 million or 4 % of the annual worldwide turnover (whichever is higher). For other violations (such as security breaches by data processors or if a data processing agreement does not meet the requirements of the GDPR), fines of up to EUR 10 million or 2 % of annual worldwide turnover (whichever is higher) could be imposed.

Though it may not be easy to enforce such imposition of fines against non-EU companies, the GDPR will definitely have an impact on such companies (including Chinese enterprises).

It is expected that the EU will issue further guidelines on the subject of penalties.

Responsibilities and sanctions under GDPR
A data processor shall be liable for the damage caused by processing where: (i) it does not comply with obligations directed to processors under GDPR or (ii) it acts outside or contrary to lawful instructions of the controller.

The GDPR has a two-tiered administrative fines:
(i) EUR 10 million or 2 % of annual worldwide turnover for violation of inter alia notification of security breach and appointment of data protection officer;
(ii) EUR 20 million or 4 % annual worldwide turnover for violation of inter alia data processing principles, consent, data subject's rights and transfers to third country.

Other important compliance matters
Other important compliance matters under the future GDPR include:

- *data protection impact assessments* (so-called 'DPIAs') for processing operations that may involve high risk for the data subjects, for example new large-scale filing systems.
- *data protection by design and default*, whereby the data controller is obliged to implement data protection measures into its IT systems and services, e.g. data minimization techniques and privacy default settings.
- *notification of personal data breach* within 72 hours of discovery and to data subjects if their rights and freedoms are jeopardized. This obligation applies only to the data controller, as data processors shall notify the data controller without undue delay of becoming aware of the breach.
- *maintaining records of all processing activities* under the responsibility of the data controller and for the data processors – all categories of processing activities carried out on behalf of a data controller. The records must upon request be made available to the relevant supervisory authority.
- *appointment of a data protection officer* for certain data controllers and processors.

Significant implications for Chinese companies

Chinese companies are currently subject to less restrictive data protection rules than EU-based companies, as China does not have a comprehensive data protection framework as that in the EU. In China, regulation of protection of personal data falls within the category of a 'right to privacy', which is governed in several sector-specific laws. The new Chinese Cyber Security Law, which came into force on 1 June 2017, shows considerable progress because it establishes a basic yet independent framework for personal information protection, but many technical measures are yet to be defined and how it would be carried out is also to be seen.

Implications for Chinese Companies
The Chinese company will also be subject to GDPR's rules on expanded territorial reach. Such Chinese companies should be aware of – among other things:
(i) The duty to appoint an EU representative
(ii) The duty to ensure that it is legal before any data is transferred to China
(iii) Failure of compliance would risk not only severe fines but also loss of reputation among business partners.

Many Chinese companies are already now subject to the EU rules on data protection. When the GDPR applies on 25 May 2018, all Chinese companies operating in or targeting or monitoring data subjects in the EU will become subject to the GDPR and will, for example, have to appoint an EU representative.

Any non-compliance with the GDPR may trigger severe fines by the applicable supervisory authority in the EU, as described above. Even though it may prove difficult for such supervisory authority to enforce such fines against Chinese companies, the GDPR will still have a great impact on Chinese companies, as EU-based companies most likely will refrain from trading with any companies that do not comply with the GDPR. If e.g. an EU-based company engages a Chinese company to deliver certain services, which entails the Chinese company processing personal data on behalf of the EU-based company, the EU-based company will risk incurring severe fines and/or being met with claims by data subjects, if the Chinese company violates the GDPR. This will be relevant for two reasons – firstly, because the EU-based company, as data controller, is ultimately liable for most of the obligations under the GDPR, and secondly, because the EU-based company and the Chinese company, as data controller and data processor, will be joint and severable liable for any claims made by data subjects.

Practical advice for Chinese companies

We recommend that any Chinese company operating in or targeting or monitoring data subjects in the EU:

- investigate whether they will become subject to the GDPR;
- form an overview of all data flows within the company/company group in order to identify whether there is a need to put in place data processing agreements, perform data protection impact assessments etc.;
- familiarize themselves with the rules and obligations in the GDPR, including the rules on international data transfers, security requirements, the rights of data subjects, etc.;
- investigate whether they have sufficient legal basis to process personal data, for instance a consent from the data subjects which fulfil the requirements of the GDPR;
- check that their privacy notices and policies meet the requirements of the GDPR, including in terms of transparency and accessibility;
- if personal data on EU data subjects are being transferred to any 'non-safe' countries outside the EU, e.g. China, then it must be ensured that such transfers are based upon a sufficient legal basis pursuant to the current regulation and in the future of the GDPR;
- ensure that protection of personal data is embedded in any data processing operations and/or IT-systems to fulfil the requirement in the GDPR of data protection by design and default; and
- put in place clear policies and procedures to ensure that they can react quickly to any data breach and notify the relevant supervisory authority and, if applicable, data subjects within the applicable time limits in the GDPR.

Kromann Reumert's Data Protection Team

Our specialists advise on all legal aspects of data protection law in all industries, including the financial sector, the research and health sector and the telecom industry, and we have reinforced and expanded our skills and advice on data protection law substantially in recent years. With our many experienced and skilled attorneys and assistant attorneys, Kromann Reumert therefore ranks among the leading Danish law firms within this field.

Data protection issues that we advise clients on include data transfers into central corporate databases, data transfers to countries outside the EU, including in connection with outsourcing, drafting and implementation of binding corporate rules, setting up whistle-blower schemes, data protection issues in relation to M&As and bankruptcies. We can help both in the obtaining of data processing permits, with enquiries and with complaints or supervisory proceedings in all of the areas listed above.

Contacts

Tina Brøgger Sørensen, Partner, tib@kromannreumert.com
Jan Ussing Andersen, Partner, jus@kromannreumert.com
Chen Chen Hu, Legal Consultant, chu@kromannreumert.com
Anna Sofia Kærsgaard, Attorney, ask@kromannreumert.com
Daiga Grunte-Sonne, Attorney, dso@kromannreumert.com

For queries in Chinese, please contact Legal Consultant
Chen Chen Hu, chu@kromannreumert.com

KROMANN REUMERT

Kromann Reumert's vision is "We set the standard". Good is not enough - we want to be the best. We provide value-adding solutions and advice with full involvement and commitment. We get there by focusing on quality, business know-how, spirited teamwork, and credibility.
We are Denmark's leading law firm, and our offices are located in Copenhagen, Aarhus and London.

COPENHAGEN
SUNDKROGSGADE 5
DK-2100 KØBENHAVN Ø

AARHUS
RÅDHUSPLADSEN 3
DK-8000 AARHUS C

LONDON
65 ST. PAUL'S CHURCHYARD
LONDON EC4M 8AB

LAWFIRM
WWW.KROMANNREUMERT.COM
TEL +45 70 12 12 11