KIRKLAND & ELLIS INTERNATIONAL LLP

KIRKLAND **ALERT**

August 2017

EU General Data Protection Regulation

Data protection laws across the EU are due to undergo "once in a generation" reforms from May 2018, including the introduction of significantly higher fines for non-compliance.

In April 2016, the EU Commission and Parliament adopted the General Data Protection Regulation (the "GDPR"). The GDPR is designed to harmonise national data protection laws across the EU, whilst at the same time, modernising the law to address new technological developments. As a regulation, the GDPR will be directly applicable, and therefore enforceable, in all 28 EU Member States as of the **25 May 2018**. Such direct effect removes the need for national implementing legislation within each EU Member State, though there will likely be some national implementing legislation as the GDPR allows for Member State discretion in certain areas, e.g., children's age. The GDPR will supersede the existing EU Data Protection Directive 95/46/EC (the "Directive") and notably has a greater extra-territorial reach. While this new legislation has been described as "*an evolution not a revolution*" of existing data protection laws, it will significantly overhaul the current EU data protection regime by introducing new concepts and approaches, the most significant of which are outlined below. Most prominently, the penalties under the GDPR are substantial and regulators are empowered to impose fines of up to *4% of total annual worldwide turnover or €20 million* (whichever is higher), depending on the type and severity of the breach.

To whom does the GDPR apply?

1. **Personal data**
   As under the current Directive, the GDPR applies to the processing of *personal data*. The GDPR defines personal data as "*any information relating to an identified or identifiable natural person*". To determine whether a person is identifiable, businesses will need to consider "*all means reasonably likely to be used*" by the business/organisation holding that data, or any other person, to identify the individual, either "*directly or indirectly*". Although this definition is broader than under the Directive (e.g., an IP address can be personal data), it largely codifies the current guidance and EU case law on the interpretation of personal data. In addition, enhanced data protection obligations are imposed in relation to processing "*special categories of personal data*" (similar to "*sensitive personal data*" under the Directive), this includes race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health data or sex life and sexual orientation, and additionally under the GDPR, genetic or biometric data.

2. **Data Controllers v. Data Processors**
   The GDPR applies to the processing of personal data by *controllers* and *processors*. The definitions of these terms are broadly the same under the GDPR as under the current Directive (i.e., controllers determine how and why personal data is processed and processors process personal data on behalf of controllers). "*Processing*" is broadly defined in the GDPR to mean any operations performed on personal data, including collection, recording, storage or transmission. One of the most significant changes introduced by the GDPR, however, is that the GDPR places direct legal obligations on data processors (in addition to data controllers) for the first time at the EU-wide level (see further below). In contrast, the Directive only imposed direct legal obligations on data controllers.

3. Extended territorial reach

The GDPR will apply to *the processing of personal data in the context of the activities of an establishment* of a data controller or a data processor *in the EU, regardless of whether the processing takes place in the EU or not* (e.g., by a non-EU affiliate or third party). Further, if your organisation is located *in a non-EU country* and has no EU presence, it will now be subject to the GDPR if it: *(i) offers goods or services to EU data subjects (even if for free); or (ii) monitors EU data subjects' behavior (*e.g., via cookies*)*. Relevant factors to assess whether businesses based outside of the EU will be caught by the GDPR include: (i) use of a currency or language used in the EU; (ii) ability to place orders in the EU; (iii) references to EU users or customers; and (iv) tracking EU residents online. In practice, this means that many companies based outside of the EU, who are targeting customers within the EU, will be subject to the requirements of the GDPR, which was not the case under the Directive. We await guidance on how this broad geographical scope will be enforced in practice.

The extra-territorial reach of the GDPR means that even certain organisations based outside the EU will be caught.

What does the GDPR mean for your organisation?

1. Substantial monetary penalties for non-compliance

Under the GDPR maximum fines for breach of data protection law will significantly increase and businesses could now face potential fines of up to the *higher* of *(i) 4% of total annual worldwide turnover or (ii) €20 million* depending on the type and severity of the breach. Notably, there is the potential for such percentage fines to be imposed on the turnover of the entire global group of companies (the interpretation of which is still to be determined), and not just the processing or controlling group entity which is in breach. Currently under the Directive, fines under national law and across EU Member States vary, and are relatively low in comparison (e.g., the maximum fine permitted in the UK is £500,000, whilst in Germany it is €300,000). This means that businesses which had previously regarded compliance with EU data protection law as presenting a relatively low risk will need to rethink their privacy law compliance strategy. The GDPR also makes it more straightforward for individuals to bring private claims against data controllers and processors. In addition, reputational damage may result from breaches of the GDPR, which is difficult to quantify.

2. Data protection principles

The data protection principles set out the main responsibilities for organisations. The principles are similar to those under the Directive, with a new accountability requirement (as discussed further below). Specifically, personal data must be:

- Processed lawfully, fairly and in a transparent manner (the "*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 (the "*purpose limitation principle*");
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "*data minimisation principle*");

- Accurate and where necessary kept up to date (the "*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 (the "*storage limitation principle*");
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organisational measures (the "*integrity and confidentiality principle*"); and
- The controller is responsible for and must be able to demonstrate compliance with the above principles (the "*accountability principle*").

To address compliance with these principles, data mapping, gap analysis and remediation action plans may need to be undertaken and implemented.

The GDPR introduces a legal accountability obligation to EU data protection law, which underpins much of the new requirements. In practice, this means that it is not enough to merely comply with the GDPR, data controllers must also be able to show how they are complying.

3. Accountability

One of the key themes of the GDPR is accountability (as above) and therefore onerous obligations have been placed on data controllers to demonstrate compliance with the GDPR. In practice this will entail (i) maintaining formal, written data processing activity records; (ii) reviewing and amending data protection policies to comply with the principles of the GDPR; (iii) conducting privacy impact assessments for higher risk processing activities; (iv) implementing technical and organisational measures to evidence the integration of data compliance measures into data processing activities (also known as "*data protection by design and by default*"); and (v) designating a data protection officer (if required). Ultimately, your organisation should be able to demonstrate its accountability and compliance with the GDPR in an organised and effective manner. The current requirement to notify an organisation's data processing practices to the UK Information Commissioner's Office (save where exempt) will fall away under the GDPR and instead detailed records of data processing activities should be kept to demonstrate compliance with the GDPR.

4. Transparency

Organisations will need to provide detailed information to individuals regarding the processing of their personal data, which must be presented in a *concise, transparent, intelligible and easily accessible* manner. The information you supply must also be written in clear and plain language and supplied free of charge. The information that you need to provide, including the timing of when such information should be provided, is set out in the GDPR, and differs depending on whether the personal data was obtained directly from the individual or not. Certain information is consistent with the current Directive, but additional information is now expressly required to be provided, including the lawful basis for processing (see further below). Further, where consent is the legal basis relied upon, separate consents will be required for different processing activities (see further below). As a result, organisations may need to amend their data protection policies and notices prior to 25 May 2018.

5. Consent

Consent is one of a number of different ways of legitimising the processing of personal data, however under the GDPR this will be harder to obtain. Unlike the Directive, the GDPR does not distinguish between what is meant by ordi-

nary and explicit consent. It instead adopts a uniform approach and proposes that consent must be *freely given, specific, informed and unambiguous*, and demonstrated either by a *statement or a clear affirmative action*. Consent must also be explicit where "*special category*" personal data is processed. Consent means offering individuals genuine choice and control. Therefore consent will not be *freely given* if consent is made a precondition of a service, or if there is an imbalance in the relationship between the individual and the controller. For this reason, consent will be particularly difficult for employers to rely on, who should look for an alternative lawful basis on which to process personal data such as "*legitimate interests*." Further, businesses which previously relied on implied consent will need to review their existing practices to ensure that any consent obtained complies with the requirements discussed above. In addition, the GDPR gives data subjects the right to withdraw consent at any time and "*it shall be as easy to withdraw consent as to give it*". Controllers must inform data subjects of the right to withdraw before consent is given. Once consent is withdrawn, data subjects have the right to have their personal data erased and no longer used for processing. The UK Information Commissioner's Office has encouraged organisations to adopt new, innovative ways of obtaining consent (such as "just-in-time" notices, layered privacy policies and icons). There are additional requirements in relation to children.

The GDPR significantly enhances the rights of data subjects and raises the bar for obtaining valid individuals' consent to processing. Organisations will need to review their policies and procedures to ensure they are equipped to support these rights.

6. Lawful basis for processing

Data subject consent is one of a number of lawful bases on which personal data may be processed under the GDPR. If a data controller does not have a lawful basis for a given processing activity (and no exemption or derogation applies) then that activity is *prima facie* unlawful. The GDPR sets out the legal bases on which personal data and special category personal data may be processed. The legal basis relied upon must be documented by the data controller and communicated to the individual (e.g., via a privacy policy).

At least one of the following conditions must be met whenever a data controller processes personal data (unless an exemption or derogation applies):

- the individual's consent;
- the processing is necessary (i) in relation to a contract with the individual; or (ii) because the individual has asked you to enter into a contract;
- the processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract);
- the processing is necessary to protect the individual's (or other persons) vital interests (i.e., life or death);
- the processing is necessary for the public interest or exercise of official authority vested in the data controller; or
- the processing is necessary for the "*legitimate interests*" of the data controller, or a third party, except where overridden by the individual's rights.

There are similarities here with the current Directive; however, certain changes introduced by the GDPR will make it harder to meet the requirements for lawful processing. For example, in addition to setting a higher standard for consent

(as discussed above), if relying on the "*legitimate interests*" basis, a controller must ensure that data subjects are informed of the legitimate interests that are being pursued, and data subjects will also have the right to object to processing on this ground.

The GDPR introduces two new mechanisms to justify international transfers of personal data outside Europe.

In order to process "*special category personal data*," at least one of the below processing conditions must be met:

- explicit consent from the individual (unless prohibited under law);
- the processing is necessary to comply with employment law / collective agreement;
- the processing is necessary to protect the individual's vital interests (where incapable of consent);
- the processing is carried out by a "not-for-profit" (and no third party disclosure without consent);
- the personal data has been manifestly made public by the individual;
- the processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
- the processing is necessary for reasons of substantial public interest (if proportionate and with appropriate safeguards);
- the processing is necessary for medical purposes (on basis of law or by a health professional);
- the processing is necessary for public health; or
- the processing is necessary for archiving purposes in the public interest or scientific or historical research or statistics (with conditions).

7. Cross-border data transfer

As under the Directive, transfers of personal data from the European Economic Area ("EEA") to third countries outside the EEA are only permitted under the GDPR where certain conditions are met (including in respect of onward transfers). In addition to replicating the existing mechanics to justify international transfers (e.g., a *finding of adequacy, the EU-US Privacy Shield, model contract clauses or binding corporate rules*), the GDPR introduces two new mechanisms for transfers outside the EEA: (i) an approved *code of conduct*; or (ii) an approved *certification* mechanism, together in each case with binding and enforceable commitments in the third country to apply these safeguards. As under the Directive, the GDPR provides for a number of narrowly interpreted derogations which permit transfers of personal data from the EEA to third countries where:

- *explicit informed* consent has been obtained;
- the transfer is *necessary* for the performance of a contract or the implementation of pre-contractual measures;

- 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;
- the transfer is *necessary* for important reasons of public interest;
- the transfer is *necessary* for the establishment, exercise or defence of legal claims;
- the transfer is *necessary* in order to protect the vital interests of the data subject where consent cannot be obtained; and
- 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 personal data where no other mechanic 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. Note that notification to the supervisory authority is required if relying on this derogation.

Unlike the Directive which places direct obligations on controllers and not processors, one of the key changes in the GDPR is that processors have direct obligations for the first time (in addition to controllers).

8. Role of Data Processors

In contrast to the current position under the Directive, under the GDPR, data processors will have direct legal obligations in respect of the personal data they process, and individuals will be able to claim compensation for unlawful processing of their personal data directly from the processor. Such obligations introduced by the GDPR include, implementing technical and organisational measures to protect personal data, notifying the controller without undue delay of data breaches and appointing a data protection officer (if required). Data controllers and processors should therefore identify their data processing agreements now so that they can review and amend as necessary, prior to 25 May 2018.

9. Data Breach Notification

Under the GDPR, data controllers will now be obligated to notify any personal data security breaches to the relevant data protection authority (the "DPA") *within 72 hours* of becoming aware of such breach, unless the breach is unlikely to result in a risk to the individual concerned. In addition, any affected individuals should also be notified of any personal data security breach, but only where an adverse effect on their privacy is anticipated as a result. Your organisation will therefore need to develop and implement a data breach response plan (which we recommend includes designating specific roles and responsibilities and training employees) enabling it to react promptly in the event of a data breach.

10. Additional data subjects' rights

Under the GDPR, data subjects will be granted additional rights, such as *the right to request that businesses delete their personal data* (i.e, the right to erasure/ "be forgotten"), *the right to access their personal data* (i.e., subject access), *the*

right to have inaccuracies corrected (i.e, rectification), *the right to prevent direct marketing*, *the right to data portability* (i.e., to transmit their personal data from one data controller to another) and *the right to object to profiling* (e.g., online tracking). As a result, businesses will need to devote additional time and resources to ensure that these issues are appropriately addressed.

Under the GDPR, controllers and processors will be regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority". The GDPR also provides for coordinated cross-border enforcement by other "concerned" supervisory authorities.

11. **One-stop shop**
    The GDPR will transform the process by which data protection laws are supervised. Currently, each data protection authority may exercise authority over businesses operating in its territory. Under the GDPR, a business will be able to deal with a single DPA as its "*lead authority*" across the EU. This means that organisations will need to identify which DPA is their lead authority, considering both the location of the business' data processing functions and the location of the company which controls the organisation's group. Businesses that operate in more than one EU Member State will see a substantial change, as the one-stop shop will mean that they predominantly interact with a single DPA as their lead authority (rather than multiple DPAs).

What is the impact of Brexit on the GDPR for the UK?

As with all other EU Member States, the GDPR will apply in the UK from 25 May 2018 and the UK Government has confirmed that the UK's decision to leave the EU by 29 March 2019 will not affect the commencement of the GDPR. The UK Government has also confirmed that there will be a new UK Data Protection Bill that will bring both the GDPR and the Data Protection Law Enforcement Directive ino UK law. The Data Protection Bill will help the UK prepare for Brexit and should put the UK in a strong position to secure unhindered data flaws from the EEA post-Brexit. The UK Information Commissioner's Office is committed to assisting organisations to prepare for the new requirements under both the GDPR and this new Data Protection Bill.

Building a road map to become GDPR compliant

As set out above, the GDPR will introduce a single legal framework that applies across all EU Member States. This means that businesses will face a more consistent set of data protection compliance obligations from one EU Member State to the next. However, the GDPR may require significant changes for many businesses, and many of these changes will require substantial time to implement. It is therefore important for businesses to plan ahead as soon as possible in order to avoid the risk of significant fines and adverse publicity. Please see below for our handy action list to begin assessing gaps in your organisation's compliance:

- ✓ **Resources and budget** — Appoint an individual (or team) in your organisation to oversee the transition and ensure that an appropriate budget has been allocated to build out new processes and policies;

- ✓ **Personal data assessment** — Assess what personal data your organisation collects and holds, where it is stored, and how it is used. Consider instructing a third party to audit your IT and security systems;

- ✓ **Third parties** — Know from whom you are collecting personal data and to whom you are transferring it. You may need to renegotiate contracts with data processors (which could take some time) and obtain clearer consent from data subjects prior to May 2018;

- ✓ **Data Processing** — Review and update any data subject consents, internal training, privacy notices, policies and data transfer mechanisms. Review existing procedures and create new ones to address restrictions on certain types of processing, such as automatic profiling, and support new data subject rights being introduced, such as data portability, enhanced data subject access requests, and the right to erasure and rectification;

- ✓ **Data Breaches** — Design and implement a data breach response plan to ensure you are able to meet the new 72-hour deadline to report sufficiently serious breaches to the relevant supervisory authority. Note that you will only have to notify the authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. Consider in advance which breaches of which personal data are likely to have this impact so that you are able to swiftly identify breaches that need to be reported;

- ✓ **Accountability** — Implement additional accountability measures (i.e., privacy impact assessments, audits and record keeping) and appoint a data protection officer (if required or desired).

If your business/organisation fails to prepare for the GDPR, it could expose your organisation to severe penalties for non-compliance.

Given the scale of the changes being introduced, and the significant potential fines attached to non-compliance, companies should prepare for compliance with the GDPR as soon as possible.

If you have any questions about the matters addressed in this *Kirkland Alert*, please contact the following Kirkland authors or your regular Kirkland contact.

Emma L. Flett
Kirkland & Ellis International LLP
30 St Mary Axe
London EC3A 8AF
United Kingdom
www.kirkland.com/eflett
+44 20 7469 2218

Jennifer F. Wilson
Kirkland & Ellis International LLP
30 St Mary Axe
London EC3A 8AF
United Kingdom
www.kirkland.com/jenniferfwilson
+44 20 7469 2474