Meeting of the DJW IT working group

Munich, February 16th 2017

The EU General Data Protection Regulation (GDPR) :

What non-EU companies need to know.

The General Data Protection Regulation is a dramatic reform of the 20 year old Data Protection regulation that is currently being used, and will apply across the European Union as from 25 May 2018. While it was created to modernise the law and streamline legal compliance for businesses with a single set of laws across the EU, the new requirements will considerably increase the regulatory burden on their controllers and processors.

What does this mean for non-EU companies? That depends on whether or not the company does any of the following:

- provide goods or services to people in the EU
- track or monitor activities or behaviours of people in the EU
- touch any data generated from individuals in the EU

If it's a "yes" to any of the above, the company will need to comply with the new regulation. Even if the company is not registered in the EU, and even the handling and or storing of the data is outsourced outside the EU, regardless, instances of non-compliance will be met with a hefty fine of up to €20 million or up to 4% or the global annual revenue.

As digitisation and data tracking are now base standard operations for any enterprise, the new regulation will have major consequences not only for the EU, but also for international businesses. However, a recent study found that companies are yet to understand the full scope of what is required for them to be compliant.

This is why for our latest DJW IT Working Group Meeting we invited Kirsten Wolgast, LL.M., Senior Associate at the acclaimed international law firm Pinsent Masons, to give a seminar on the key changes to the Data Protection, and also answer questions from the audience. The Q&A session proved to be most enlightening, as it shed light on the scope of work companies will need to undertake in order to be ready for the regulation by next year. While the seminar was given from the perspective of Brexit, and the implications for UK based companies or companies with ties to the UK, the information applies to international businesses in general. Below are some of the notes taken from the meeting.

Key points to note in the GDPR

- **Expanded definition of 'personal data'** – this has been broadened to cover any information related to identified or identifiable living individuals. Specific definitions have been introduced for genetic data and biometric data, as well as for the concept of 'pseudonymisation' and 'anonymous information' (Article 4).

- **Right to be forgotten** – users can request that their personal data be deleted, including links to and copies of that personal data (Article 17).

- **Data portability** – users can ask for a copy of all their data, and you must be able to provide it in a "structured, commonly used and machine-readable format" (Article 20).

- **Security breach notification** — mandatory "personal data breach" notifications to the supervisory authority without undue delay (within 72 hours where feasible) (Article 33), and personal data breach notifications to the data subject without undue delay where there is a high risk to their privacy (Article 34).

- **Data protection impact assessments** – before initiating any processing likely to result in a high risk to individuals (such as profiling activities) controllers will have to carry out a review of that envisaged processing to assess the privacy risks to individuals(Article 35), and consult with the supervisory authority in some circumstances (Article 36).

- **Data protection officers (DPO)**: companies that conduct large-scale monitoring or large-scale processing of sensitive data or data on criminal convictions as core activities must appoint a DPO. A DPO must operate independently and must not take instructions from his employer (Article 37)

- **Privacy by design and by default:** each new service or business process that makes use of personal data must be able to demonstrate that they have adequate security in place and that compliance is monitored. Furthermore, the strictest privacy settings must be automatically applied once a customer acquires a new product or service (Article 25).

- **Tighter rules on international transfers** – restrictions on transferring personal data outside the EEA (eg to data centres or accessing remotely from outside EEA) will generally be tightened up. As before, 'adequate data protection level' must be provided by the data importer itself or the data importer's country.

- Note that for top tier breaches, administrative fines will be issued to the maximum of 20 million euro or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise.

- Especially important for non-EU companies, a breach in the international transfer rules is considered a top tier offence.

Q&A

Audience Question: How do data protection laws in Japan compare to the GDPR?

Ms Wolgast: The Japanese data protection laws are not deemed as meeting the required threshold of 'adequate level of protection', meaning a level of data protection comparable to the GDPR, i.e. in case of a transfer of data from the EEA to Japan, it has to be ensured that the Japanese data importer provides for an 'adequate level of data protection'. Furthermore, Japanese companies will have to adhere to the GDPR where relevant.

Audience General Comment: The right to be forgotten is a huge burden for us. We didn't have this concept when the data base was built, and so it's difficult for us to identify where the data is located.

There's also the problem with definition – which fields are personal, which fields are not. For example, in the health insurance sector, the fact that the individual has insurance with our company is in itself considered personal data.

Audience General Comment: for our company (leading international IT services enterprise), our first big task is also to figure out "where are the data?". We need to create a mapping system to identify where they are globally, and within systems, and to see what's critical.

Audience Question: For the right to portability, is there a common format, or a standard platform? Do we just give current info, or all interactions that the customer has had with us – for example, recordings of phone conversations to our call centres?

Ms Wolgast: The format needs to be machine readable, but there's no indication that a platform will be provided.

Question from Ms Wolgast to audience: Do you think it will be easy to identify the data flow of transfers, or difficult?

Audience Comment: This will be a big issue. We have certain IT service offices and data centres that do our data processing in the UK.

Audience Question: If our physical server is in the EU, and we outsource the data processing to outside the EU, will it still need to follow the GDPR.

Ms Wolgast: Yes. When someone outside the EU is accessing data in the EU, this is an international data transfer, which is covered under the GDPR.

Final notes

We would like to thank Ms Kirsten Wolgast once again for the illuminating seminar, and for the interesting discussions that it generated.

For further detailed reading, here is downloadable a GDPR guide from Pinsent Masons (written in from a Brexit perspective for UK companies, but the information applies also to international enterprises).

https://www.pinsentmasons.com/PDF/2016/Brexit/General-Data-Protection-Note-July-2016.pdf

And here is an archive of articles on the topic posted by Pinsent Masons:

https://www.pinsentmasons.com/en/search-results/?terms=gdpr

recent study found that companies are yet to understand the full scope:

http://blog.isc2.org/isc2_blog/2017/01/emea-gdpr-warning.html

Kirsten Wolgast

https://www.pinsentmasons.com/en/people/senior-associates/kirsten-wolgast1/

Pinsent Masons

https://www.pinsentmasons.com