Uber Arrogance, "God View" and Data Protection.

- Published on August 18, 2017

Noel Doherty
IT and Data Protection, Employment and Family/Child Care, Solicitor, Collaborative Lawyer at FitzGerald Solicitors

Breach of data protection and privacy laws by Uber, the ride sharing company in the United States.

The “God view” tool employed by Uber allowed the company’s employees to constantly track drivers and customers in real-time without their knowledge. In 2011 the “God view” programme was used by Uber as a type of novelty feature at their launch parties, as they extended their business to different cities in the United States, by giving examples of real-time location tracking of well-known local individuals.

In 2014 the New York Attorney General reached a settlement with Uber imposing a fine of $20,000. A minor slap on the wrist for a company with a turnover size of Uber’s. Uber assured lawmakers that it would restrict and monitor employee access to the programme.

It now transpires that Uber rarely monitored how employees were using “God view” and that they failed to implement basic security practices to protect customers’ and drivers’ privacy. The Federal Trade Commission in the United States has now imposed an obligation on Uber to hire an outside firm to audit its privacy

practices every two years for the next two decades but has not imposed a monetary fine.

The General Data Protection Regulation, **" GDPR "** will come into effect in all EU countries on 25 May 2018. In the event that Uber were proven to have engaged in the same practices as have been disclosed in the United States, the powers granted to the proposed new Data Protection Commission could result in fines of up to **€20 million or 4% of total worldwide annual** turnover whichever is greater.

Penalties of that magnitude will hopefully discourage the type of breaches of customer and employee privacy demonstrated at Uber. All organisations holding personal data in respect of customers and employees will need to ramp up their systems to ensure compliance with GDPR. Data controllers and data processors will need to put in place data protection impact assessments, guarantee and record elevated thresholds for consent, report security breaches promptly and retain comprehensive records in respect of the personal data held and the uses to which it is put.

Individuals should make themselves aware of their rights under the GDPR and organisations must ramp up their policies and procedures concerning data protection and privacy.

Noel Doherty, Solicitor. Fitzgerald solicitors Cork.