VORYS

Publications

Client Alert: EU Privacy Officials Release Guidance on Data Breaches, Profiling

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 10.19.2017

On October 17, 2017, the European Union (EU) Working Party on The Protection of Individuals with Regard to the Processing of Personal Data (also referred to as the Article 29 Data Protection Working Party) released two draft guidance documents. One provides guidelines on when to notify regulators and individuals about personal data breaches while the other provides requirements for automated data processing that may profile individuals. Both guidance documents relate to requirements under the General Data Protection Regulation (GDPR), the new EU privacy regime set to take effect in May 2018.

The draft guidance on breach notification explains that not all security incidents are necessarily personal data breaches triggering notification obligations. The draft guidance also expands what it means to be "aware" of a breach by saying that the data controller, the company which controls the collection and use of data, should be considered to become aware of a breach only when it has a reasonable degree of certainty that a breach that compromised personal data has occurred. The GDPR also requires companies that process data notify the data controllers that ordered the processing of data breaches. Under the draft guidance, the data controller would be considered to be aware of the breach as soon as the processor's notice is received, thereby triggering the 72 hour period for the data controller to notify the appropriate authorities.

The GDPR grants data subjects the right to object to decisions made about them when the decision is based solely on automated decision-making. For example, an individual could challenge a decision not to grant them a loan if that decision is made only on the basis of automated credit scoring. Under the draft guidance on profiling, in such situations, the data controller must provide an easy way for data subjects to object to automated decision-making and contest the decision at issue. Furthermore, the draft guidance notes that human involvement is necessary in a review of automated decision, along with any additional information provided by the data subject. Entities controlled data of EU residents should heed the guidelines under the draft guidance as violations of prohibitions on profiling and automated

decision-making can lead to a hefty fines.

For questions related to EU privacy and breach response, please contact Nita Garg, Jonathan Ishee or your Vorys attorney.