SQUIRE PATTON BOGGS

Weekly Data Privacy Alert

12 June 2017

EU

Latest Report on Effect of GDPR Predicts Heavy Consequences for Financial Services Sector

Consult Hyperion, as commissioned by All Clear ID (experts in data breach solutions), has published a new report focussing on the effect of the GDPR on banks. The report states that the highest risk item for banks is the breach notification requirement, which requires data controllers to notify a supervisory authority of a personal data breach no later than 72 hours after becoming aware of it. They must also provide detailed information regarding the breach, such as the approximate number of data subjects and records affected and the nature of the personal data breach. The penalty for non-compliance with this requirement under the GDPR can be up to €10 million or 2% of global annual revenues. Further, the report forecasts that European banks can expect fines in the region of €4,662 million in the first three years after the introduction of the GDPR (excluding compensation claims, costs associated with lost customers, damaged reputations and senior executive resignations). One reason for this identified by the report is that the chances of a breach occurring will likely increase due to the requirements of other European financial service regulations simultaneously coming into force and increasing the scope and longevity of personal data (the ePrivacy Regulation, the Anti-Money Laundering Directives and the Second Payment Services Directive).

France

The CNIL Issues Fine to Dental Practice in Relation to Access Right and Lack of Cooperation With the DPA

On 18 May 2017, the CNIL issued a sanction in the form of a fine of €10,000 against a dental practice for breach of its patient's right to access its file and for lack of cooperation with the CNIL during the investigation process. Indeed, the dental practice had not responded to its patient's request to obtain its personal information by accessing its file and subsequently failed to respond to the CNIL's five letters requiring it to comply with data protection laws.

UK

ICO Fines Council £100,000 for Failing to Adequately Prevent a Cyberattack

Yet another council has been fined by the ICO for failing to comply with data protection laws. This time, it is the Gloucester City Council that left personal information vulnerable to a cyberattack, despite warnings from the ICO. An attacker accessed the council's website in July 2014 and downloaded over 30,000 emails that contained financial and sensitive information about council staff. The ICO investigation found that the council did not have sufficient processes in place to ensure compliance with data protection laws and therefore issued a fine of £100,000.

Contacts

Philip Zender
Partner, San Francisco
T +1 415 393 9827
E philip.zender@squirepb.com

Francesca Fellowes
Senior Associate, Leeds
T +44 113 284 7459
E francesca.fellowes@squirepb.com

Stephanie Faber
Of Counsel, Paris
T +33 1 5383 7400
E stephanie.faber@squirepb.com

Annette Demmel
Partner, Berlin
T +49 30 7261 68 108
E annette.demmel@squirepb.com

Caroline Egan
Consultant, Birmingham
T +44 121 222 3386
E caroline.egan@squirepb.com

Emma Garner
Associate, Leeds
T +44 113 284 7416
E emma.garner@squirepb.com