Summary Final Decision Art 60

Legal Obligation

Administrative fine

EDPBI:UK:OSS:D:2020:154

Background information

Date of final decision:	30 October 2020
Date of broadcast:	30 October 2020
LSA:	UK
CSAs:	All SAs
Legal Reference:	Personal data breach (Articles 33 and 34), Security of processing (Article 32)
Decision:	Administrative fine
Key words:	Administrative fine, personal data breach

Summary of the Decision

Origin of the case

The controller for the data processing activity at stake acquired a company whose IT systems were infiltrated by an attacker before the acquisition. The controller was not aware of the infiltration during the acquisition, nor became aware of this afterwards. The controller became aware of the infiltration once the attacker triggered an alert in relation to, among others, a table containing cardholder data. The attacker appeared to have obtained personal data in both encrypted and unencrypted form. The unencrypted personal data contained data from the guest profile**s**, including reservation information, while the encrypted information contained 18.5 million encrypted passport numbers and 9.1 million encrypted payment cards. Subsequently, the controller promptly informed the data subjects and took immediate steps to mitigate the effects of the attack. Finally, the controller notified the LSA of a personal data breach.

Findings

The LSA investigated the case and found that the controller did not ensure appropriate technical and organisational measures to ensure an appropriate level of security as required by Article 5(1)(f) and Article 32 of the GDPR. In particular, the LSA found that the controller did not sufficiently monitor the

privileged accounts and the databases. In addition, the LSA also found that the controller failed to ensure that the actions taken on its systems were monitored appropriately and that the controller did not, in some instances, apply encryption to all the passport numbers and other categories of personal data.

Decision

The LSA, considering the relevant mitigating factors, imposed an administrative fine of £18.4 million on the controller.