VERDICT

# Bupa fined for inadequate security following theft of customer data

## Insurance and healthcare group Bupa has been fined £175,000 for failing to protect customer data after an employee attempted to sell personal data of 547,000 Bupa customers on the dark web.

The Information Commissioner's Office (ICO) found that Bupa did not put effective security measures in place to protect customers' personal information.

The former Bupa employee behind the breach sent bulk data reports to his personal email between January and March 2017 from the company's customer relationship management (CRM) system, which has records of some 1.5m customers.

The data contained names, birth dates, email addresses and nationalities of customers.

### Bupa breach discovered

An external Bupa partner saw the customer data for sale on the dark web and alerted Bupa in June 2017.

Bupa and the ICO received 198 complaints about the incident, which led to the employee's dismissal and Sussex Police issuing a warrant for his arrest.

Despite the scale of the breach, the ICO found Bupa had failed to routinely monitor its CRM system's activity log and so had not detected any unusual activity.

The timing of the case meant that Bupa was charged with breach of the Data Protection Act 1998 rather than the General Data Protection Regulation, which replaced it in May 2018. As a result, the ICO was only able to impose a fine of up to £500,000.

Under new GDPR laws, companies that fail to adequately protect data face a fine of up to €20m or 4% of global annual turnover, whichever is greater.

## Inadequacies in Bupa's safeguarding of personal data

ICO Director of Investigations, Steve Eckersley, said:

> "Bupa failed to recognise that people's personal data was at risk and failed to take reasonable steps to secure it.
>
> "Our investigation found material inadequacies in the way Bupa safeguarded personal data. The inadequacies were systemic and appear to have gone unchecked for a long time. On top of that, the ICO's investigation found no satisfactory explanation for them."

Director of Legal Services at ThinkMarble Robert Wassall said:

> "This breach, which took place over a period of about two months before it was discovered, is another case of a personal data breach being caused by the deliberate and malicious actions of an employee.
>
> "What businesses in this position now will have to consider is the effect of the GDPR when dealing with such insider threats. Under GDPR, if Bupa had been found in breach based on this inaction, based on its turnover to December last year of £490,413,000, it could have been issued a maximum fine of 4% of turnover, £19,616,520."

Chief Information Security Officer at ThinkMarble Jim Palmer added:

> "This breach, as the ICO says, was caused by systematic failures and it would be interesting to know if Bupa had any external processes to test and check its security arrangements in place. The fact that the breach was discovered only due to the vigilance of a third party indicates that Bupa did not have in place appropriate technical security measures as required by GDPR Article 32."