The new data protection policy came into force on 25th May 2018 and many companies have already experienced its knock-on effects. Review the Yahoo case and make sure you aren't the next to be fined.

Recently, the British Information Commissioner's Office fined Yahoo for failing to comply with the Data Protection Act of 1998. The reason - the leakage of 500 thousand UK citizens' personal data in 2014.

How It Happened

In 2014, cybercriminals cracked Yahoo's servers and stole the credentials of half a million users, including dates of birth, phone numbers, passwords, account recovery questions and their answers. The theft was uncovered after a man using the nickname "Peace", known for the "dump" of LinkedIn and Myspace user data, began offering the Yahoo database for sale for only 3 bitcoins. The announcement appeared in the Darknet in 2016, but the hacker said that he had already stolen some of the data back in 2012 and was selling it in secret.

During an investigation involving the FBI, it turned out that Yahoo were aware of the attack immediately after it occurred, but preferred to remain silent until September 2016. Under the new GDPR, organisations are forbidden from hiding leaks from the public for so long. Articles 33 and 34 of the regulation oblige organisations to notify the data owners and supervisory authorities within 72 hours of the discovery of a leak. The GDPR imposes multi-million-dollar fines for non-compliance (art. 83, para. 4).

In this case, Yahoo is accused of:

- Failing to ensure the safety of 515 121 users' data;
- Failing to process personal data in the manner required by the regulations;
- Failing to report any detected "holes" or leaks for a significant length of time.

As a result, the British Information Commissioner's Office decided that Yahoo was in violation of Part 1 of Section 7 of the DPA 1998, which refers to "*the need to take appropriate technical and organisational measures to prevent unauthorised or illegal processing of personal data, as well as its accidental loss, damage or disposal* ". According to sec 55A DPA 1998, the maximum penalty in this case is £500 000. The Office took into account the mitigating circumstances (listed on page 12 of paragraph 44 of the the Yahoo case ruling, in which the Commissioner highlighted the company's willingness to cooperate with government officials and the complexity of cyber-attacks); however, the fine levied against the company cannot be avoided.

Here at Magora, we discussed GDPR compliance during the webinar with our business consultant Dmitry. Find out how you can automate data processing and download our checklist to double-check whether you've covered all the risks.

Download the Checklist

What's Next

James Dipple-Johnstone, deputy operations commissioner for ICO, in his post dedicated to the Yahoo case, notes that people entrust companies with their data hoping that their personal information will be in safe hands and will not be transferred to third parties. Unfortunately, not all organisations take data protection seriously. In such conditions representatives of the law are forced to take up the case.

The Office understands that cyber attacks are inevitable and will continue, while cybercrime will become more sophisticated, but they require companies to do their best to protect their clients' data.

As for us, we can offer the power of high technologies to help you optimise core business and data processing operations to guarantee the highest level of data security and flawless workflow - or investigate the steps you can take to increase your company's ROI via bespoke enterprise development.

Software development and automation can save you from many headaches, including potential GDPR-violation penalties. Don't wait till you need a lawyer - drop us a line to discuss your issue.