Information Commissioner's Office

The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

To: Optionis Group Limited

Of: Kd Tower, Cotterells, Hemel Hempstead, Hertfordshire, HP1 1FW

The Information Commissioner (the Commissioner) issues a reprimand to Optionis Group Limited ('Optionis') in accordance with Article 58(2)(b) of the UK General Data Protection Regulation in respect of certain infringements of the UK GDPR.

The reprimand

The Commissioner has decided to issue a reprimand to Optionis in respect of the following infringements of the UK GDPR:

- Article 5(1)(f) which states:

  "*personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*".

- Article 32(1) which states:

  "*taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*."

The reasons for the Commissioner's findings are set out below.

- Optionis did not have appropriate organisational measures in place to ensure the confidentiality and integrity of their systems. Optionis had no clear Bring Your Own Device (BYOD) policy, and an inadequate account lockout policy. The National Cyber Security Centre ('NCSC'), recommends having appropriate account lockout[1], and a BYOD policies[2] in place. Had these elements been addressed sooner, it could have significantly reduced the likelihood of a successful attack.

- Optionis did not have multi-factor authentication ('MFA') in place for the affected user account. Extensive guidance was available via the NCSC which promoted the use of strong or multi-factor authentication.[3] Additional means of authentication serve to make unauthorised access more difficult and help to protect particularly sensitive or private personal data.

Aggravating factors

In the course of our investigation we have noted that Optionis held personal data for longer than was necessary. We have also noted that Optionis took 11 months to notify all individuals of the breach. Optionis explained that the analysis of the impacted personal data took a considerable amount of time to complete, in particular, due to the size of the dataset.

Mitigating factors

In the course of our investigation we have noted that the Covid-19 pandemic would have led to Optionis having to respond quickly to allow colleagues to work from home. The work from home arrangements had been in place for approximately 2 years before the incident took place, therefore, we did not consider the Covid-19 pandemic a sufficient mitigation to lower the level of regulatory action.

Remedial steps taken by Optionis

The Commissioner has also considered and welcomes the remedial steps taken by Optionis in light of this incident, in particular:

- Correcting all underpayments to individuals by 6 February 2022.

---

[1] Password policy: updating your approach - NCSC.GOV.UK
[2] Bring your own device (BYOD) - NCSC.GOV.UK
[3] Multi-factor authentication for online services - NCSC.GOV.UK

- Commissioning a third-party cyber security firm to investigate [redacted] this incident and liaising with its IT consultants for advice and assistance with remedial measures.
- Implementing a comprehensive set of policies to protect and control the security of personal data.
- Deploying 24/7 Managed Detection and Response (EDR) covering all corporate devices.
- Enabling multi-factor authentication (MFA) on user accounts.
- Enforcing conditional access on user accounts.

Decision to issue a reprimand

Taking into account all the circumstances of this case, including the aggravating factors, mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to Optionis in relation to the infringements of Article 5(1)(f) and Article 32(1) of the UK GDPR set out above.