Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

24 August 2023

Case Reference Number: INV/0119/2022

Dear [redacted]

Thank you for your recent response on behalf of the Morgan Hunt Group.

This case has been considered under the UK General Data Protection Regulation (UK GDPR) due to the nature of the processing involved.

Our consideration of this case

After careful consideration of all of the information that you have provided to us, we have decided not to take any formal regulatory action on this occasion.

This decision is due to the particular facts of this case and the remedial measures you have taken following the incident.

Please note, if you become aware of any further information relating to this incident which significantly increases the level of risk or detriment to individuals, it is a requirement that you provide the ICO with an update. You can do so by replying to this email. If any further incidents are reported to us, we will revisit this matter and regulatory action may be considered as a result.

Further Information

Article 32 of the GDPR states "*the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".* In line with this, we have outlined some additional information below which can assist you in assessing and mitigating the risks of unauthorised access.

First, we would like to remind you of the importance of assessing the likely risks to individuals as a result of a personal data breach and maintaining a continual assessment of the incident and associated risks, especially as and when more data comes to light. Where high risk is determined, you must communicate the breach to affected individuals without undue delay. Prompt notification will enable individuals to take steps to protect themselves from the effects of a breach and help to mitigate any potential damages. The UK GDPR explains the types of damages that can occur where a personal data breach, if not addressed in an appropriate and timely manner, which includes identity theft or fraud, financial loss, loss of control over personal data and limitations of an individual's rights.

The UK's National Cyber Security Centre (NCSC) has published risk management guidance to help organisations make key decisions about cyber security risk. This may assist you in overseeing the risks to your organisation and demonstrating accountability of decisions you make with regards to security.

[redacted]

We would also like to draw your attention to the NCSC's guidance on supply chain security, which covers the importance of understanding the security risks, identifying the level of protection required and establishing control over a supply chain. The NCSC specifically recommend that an organisation should set minimum security requirements for suppliers which are justified, proportionate and achievable.

[redacted]

[redacted]

Finally, we would recommend reading our GDPR security guidance and guide to IT security to assist you in protecting the personal data within your systems in line with the relevant policies and procedures you have in place.

Thank you for your co-operation and assistance during the course of our investigation. We now consider this matter to be closed.

Yours sincerely,

Laura Jones
Lead Technical Investigations Officer
Information Commissioner's Office
Direct dial number: 0330 313 1872

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the UK General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes basic details about the complaints, investigations and self-reported data breaches it handles. These details include the name of the organisation concerned, the dates that we opened and closed the case, and the outcome. Examples of published data sets can be found at this link: Complaints and concerns data sets | ICO.

We do not include personal data in the published datasets and will anonymise the names of sole traders etc prior to publication. We also do not publish cases concerning domestic CCTV complaints and may not publish certain other cases if we feel it is not appropriate to do so in the circumstances.

If you wish to raise an objection to us publishing a case in the datasets, whether or not we have published it yet, please contact us explaining your reasons for this at accessicoinformation@ico.org.uk. We will only agree to this in limited circumstances where we are satisfied that the interests of the parties involved would override the ICO's obligations to publish this information.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice