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

[redacted]

By email only to: [redacted]

31 October 2019

Dear [redacted]

RE: Investigation of incident of 18 February 2019

I write to inform you that the ICO has now completed its investigation into the theft of personal data in relation to [redacted] customers.

In summary, it is my understanding an individual who had previously been employed by [redacted], and had legitimate access to [redacted] data held on the [redacted] portal exported unauthorised data. The [redacted], [redacted], a [redacted] were engaged on your behalf as data processors.

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

Based on the information you have provided, we have decided that regulatory action is not required in this case. The reasons for this are below.

Our consideration of this case

I have investigated whether [redacted] has complied with the requirements of data protection legislation.

In the course of my investigation I have noted that the [redacted] portal had a weak password and the ability to mass export data.

However, in the course of my investigation we have noted that the incident occurred due to a deliberate act of an ex-employee who used information that had been legitimately gained through his employment with [redacted] with the intention of extracting money from [redacted]

[redacted] had the relevant contracts in place with [redacted] and [redacted] as their data processors, which provided sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will

meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

There has been no damage or distress to any of the data subjects involved in this incident and you have not received any complaints as a result of the infringement.

We also welcome the remedial steps taken by [redacted] in light of this incident. In particular that you immediately took down the portal and following an investigation found vulnerabilities with 2 other portals which were not operating to the agreed standard and you also took those down. You contacted the affected data subjects informing them of the incident and told the data subjects to be vigilant in relation to phishing emails

Therefore, after careful consideration and based on the information provided, we have decided not to take any formal enforcement action in this case.

Further Action Recommended

The Commissioner considers that [redacted] needs to take certain steps to improve compliance with GDPR. In particular:

1. Consider more regular reviews of any 3rd parties you engage to ensure they are meeting their contractual agreements in relation to compliance with data protection legislation including having appropriate technical and organisational measures, confidentiality and the processing of data only on your documented instructions to ensure the protection of rights of data subjects.

2. Consider how to improve password management with your providers, an area you have already identified.

Please note that if further information relating to this incident comes to light, or if any further incidents involving [redacted] are reported to us, we will revisit this matter, and enforcement action will be considered as a result.

Further information about compliance with the GDPR can be found at the following link.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely

[redacted]
Lead Case Officer
Investigations
Information Commissioner's Office
[redacted]

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 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 the outcomes of its investigations. Examples of published data sets can be found at this link (https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

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