From:
Sent: Tue, 12 Feb 2019 08:11:00 +0000
To:
Cc:
Subject: CAMS-012-33955459-8 Response to Personal Data Breach Notification -ICO[Ref. COM0793415]

From: casework@ico.org.uk [mailto:casework@ico.org.uk]
Sent: 05 February 2019 07:52
To:
Subject: CAMS-012-33955459-8 Response to Personal Data Breach Notification - ICO[Ref. COM0793415]

5 February 2019

Case Reference Number COM0793415

Dear

I am writing further to your personal data breach report regarding the unauthorised disclosure of personal data when failing to redact information provided as part of an FOI request.

Thank you for the information you have provided.

Data security requirements

You are required to have appropriate technical and organisational measures in place to ensure the security of personal data.

Our Decision

We have considered the information you have provided and we have decided that no further action by the ICO is necessary on this occasion. This decision is based on the information we have recorded about the breach.

The reasons for our decision are as follows:

- The personal data disclosed was limited to the basic personal identifiers of professionals and adults. No information about the young person, any criminal convictions, or special category data was included in the breach. Additionally, you have not advised that any address or

contact details were given for any of the named individuals, making any unwanted contact or harassment unlikely.
- You believe the risk to the affected data subjects to be minimal and have not reported any actual harm having been caused, in your initial report, or at any time since the incident occurred.
- The information provided to the FOI requestor was published online. You immediately contacted the website owners and arranged to have this removed and provided the requestor with a suitably redacted copy of the form.
- The staff members responsible for the incident received recent data protection training and you intend to supply follow-up training in response to the incident.

I am sure that you can appreciate that an error such as this can lead to significant consequences for data subjects if special category data or sensitive circumstances were involved and could, if not addressed, lead to regulatory action for data controllers if future breaches occur.

It is of particular concern when these breaches occur where a data controller is dealing with highly sensitive or special category personal data, or where the individuals are vulnerable. The greater the risk that any personal data poses to individuals, the greater the security measures that should be put in place.

We recommend that you investigate the causes of this incident to ensure that you understand how and why it occurred, and what steps you need to take to prevent it from happening again.

In particular, we recommend that you consider:

- Reviewing your policies and procedures to ensure that practical and detailed guidance is given to staff regarding the correct execution of their day to day roles.
- Implementing mandatory checks and safeguards to be carried out prior to responses being sent. It is helpful to have these clearly written into your policies and procedures.
- Providing feedback to all staff about the nature of the breach and the potential impact this may cause as well as reiterating their legal obligation, under GDPR, to protect personal data.
- Reviewing the content of your data protection training to ensure that it covers practical examples of data protection in practice and that it is tailored to staff roles. It would appear from your report that staff may benefit from more detailed training in suitable redaction practices.

- Undertaking a review of all policy documents, blank forms or other material which may have been completed in a similar fashion, to ensure that only blank copies are held. Where personal data has been entered into these forms, staff should ensure that they have used an appropriate file name and storage location to distinguish templates from completed documents.
- You have stated that you contacted the website to request removal of the form and that you provided a redacted version to the requestor but have not stated whether you instructed the requestor to delete all copies of the personal data sent in error. If this is not the case you should ensure that you receive confirmation that no unauthorised personal data is held by the individual and that they have not further shared, copied or disseminated it in any way.

Please note that we may make additional enquiries if we become aware of new information which affects the circumstances of this case.

Thank you for reporting the incident. Further information and guidance relating to data security is available on our website at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

We now consider the matter to be closed.

Yours sincerely

Lead Case Officer

For information about what we do with personal data see our privacy notice

--