

Email

From  ICO Casework

To 

Cc

Subject ICO Decision - IC-248937-K3Y2

Display Name

Date Received 02/08/2023 15:36

Email Address

Reference Number IC-248937-K3Y2
Your reference: RM23044908

Dear ,

I am writing about the personal data breach report you submitted on 1 August 2023.

Thank you for the information provided.

Data security requirements

It is important to have appropriate technical and organisational measures in place to ensure the security of personal data.

Our decision

We have considered the information provided and we have decided not to take action. This decision is based on the information we have recorded about the breach.

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

We deal with thousands of personal data breach reports each year. In many cases, the breach could easily have been prevented. Please read our attached leaflet, which contains our tips for preventing the most common personal data breaches. If you're not doing these things already, please consider implementing them.

We also recommend you check that your policies and procedures are fit for purpose. All staff who handle personal data should receive regular data protection training. If you haven't already done so, you should implement any specific steps you identified to prevent a recurrence of this incident.

I note from your report that there was a delay in notifying the ICO of this breach. It is important to report to the ICO within 72 hours of becoming aware of the incident. Additional information can be provided at a later date.

Please note that we have added a new Breach Report form to our website. This should be used going forward when you report any personal data breaches to the ICO.

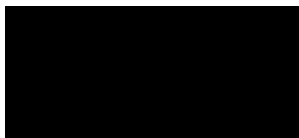
Thank you for reporting the breach. Further information and guidance relating to personal data breaches under the UK General Data Protection Regulation (UK GDPR) and data security is available on our website at:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

<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



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

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF


T. 0303 123 1113 ico.org.uk twitter.com/iconews

Please consider the environment before printing this email

Please be aware 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 data protection laws and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk). Please say whether you consider any of the information you send us is confidential. You should also say why. We will withhold information where there is a 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

ATTACHMENTS

File Name	Followed	File Size (Byte...)	
Personal Data Security Leaflet - Pre...	No	28,674	
1 - 1 of 1 (0 selected)		Page 1	

Personal data security: how to prevent some common personal data breaches in the Police and Justice sector

1. Send electronic information securely

Wherever possible, make sure to password protect or encrypt any sensitive documents sent via email. This reduces the risk of the wrong person being able to access the information. Make sure you send the passwords for electronic documents in a separate email.

2. Use secure postal delivery

If you need to need send documents by post, you should think about using recorded or tracked delivery. This reduces the risk of information being lost in the post and, if there's an issue with the delivery, you can carry out more effective searches.

3. Store hard-copy information carefully

It's important to make sure any hard-copy documents are kept secure; this applies equally whether you are in the office or on the move. Where you're using paper records, these should be kept in locked cupboards or filing cabinets. If you are on the move you should consider whether you need to be taking paper records out of the office or whether these can be kept electronically. If it is absolutely necessary to carry paper records, ensure these are kept in sight at all times and should not be left unattended.

4. Protect your devices

Devices holding personal data should be password protected and, where possible, encrypted. Encrypting devices containing provides effective protection against unauthorised access by a third party. You should use encrypted communications channels when transmitting any personal data over an untrusted network. Any removable storage devices like USBs or CDs should be kept in a safe place when they are not being used.

5. Check the accuracy of the information you hold

You should make sure that personal data is recorded accurately on your systems. Personal details such as postal addresses and telephone numbers should be kept up to date and any old or incorrect information should be removed. This reduces the risk of personal data being sent to an incorrect recipient.

6. Keep awareness of data protection high

You should make sure that all staff have received appropriate data protection training, which is tailored to their job role. We recommend that refresher training is carried out annually. However, you can also issue regular data protection reminders via emails, internal bulletins or team meetings.

7. Avoid inappropriate access

It is likely that your staff will need access to personal data in order to fulfil their role, and some of this data may be sensitive. You need to provide clear advice about what they should and shouldn't do with the personal data they have access to. You should also consider whether access controls and passwords should be added to certain documents or folders.

8. Carry out quality assessment checks

If you make a change to one of your established processes, carrying out quality assessment checks to confirm staff understanding and collect feedback can be really helpful when it comes to avoiding future mistakes.

9. Label documents clearly

Whether you hold documents electronically or physically, it's important that they're labelled clearly with appropriate titles. This helps to reduce the likelihood of information going missing or being viewed by those who are not required to see it.

10. Keep your IT systems up-to-date

You can reduce your risk of cyber threats, such as attacks on computer systems, by making sure you regularly install security updates. The guidance issued by the National Cyber Security Centre (NCSC) can help you to prepare for and deal with cyber security incidents you may experience. You can find out more through their website:

<https://www.ncsc.gov.uk/>