Upholding information rights

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

[redacted]
Probation Board for Northern Ireland (PBNI)
Communications Unit (Compliance)
80/90 North Street
Belfast
BT1 1LD

By email only to: [redacted]

19 May 2022

Dear [redacted]

Case Reference Number INV/0864/2021

I write to inform you that the ICO has now completed its investigation into the incidents when calendar WebEx invites, containing WebEx joining instructions for online programmes, were sent as group calendar invites through Outlook to service users. The email addresses were visible to other recipients. The service users are obliged to provide their contact details to PBNI to ensure adherence to their Court Order for maintaining contact with their Probation Officer and in relation to the programmes they are required to attend.

In summary, it is my understanding that this happened on three separate occasions relating to the Horizon programme (for service users convicted of sexual offences) and programmes for users convicted of domestic violence. In total 27 service users had their email addresses revealed to other recipients.

This case has been considered under the Data Protection Act 2018 (the DPA 2018) due to the nature of the processing involved.

Our consideration of this case

We have investigated whether PBNI has complied with the requirements of data protection legislation.

In the course of our investigation it has been noted that:

- The majority of email addresses involved contained identifiable attributes to individuals being made up of either the full name or part of their name. In addition, further research on any of the email addresses may also have allowed for a person to be identified via links to social media sites or similar.

- Whilst there was no other personal data revealed apart from the email addresses, a recipient of these emails could infer that the other names in the group had been convicted of domestic violence or sexual abuse and therefore there is a risk of damage or distress to the data subjects.
- The WebEx system, as used for internal meetings, was not the most secure way to invite this group of individuals. PBNI did not implement sufficient measures to identify the risks in delivering the online programmes and specifically how to invite attendees. The same system was used to invite the service users as was used for staff meetings and sufficient considerations were not put in place to prepare for how invitations to potential attendees were to be sent.
- Whilst PBNI completed a recovery plan, a DPIA was not conducted in relation to running the programmes online and the risks were not thoroughly evaluated.
- There was mandatory staff training about GDPR in 2018 but no mandatory element since for all staff. However, since the incidents the online training video has been made mandatory for all staff.

We have also considered the following in mitigation:

- PBNI staff have been working in a hybrid way (a combination of home and office working) since March 2020 due to the Covid-19 pandemic. Prior to the introduction of online programmes staff in PBNI would not have sent any external group emails to service users. The need for programmes to be delivered online was as a direct result of social distancing regulations and decisions had to be taken as to how to facilitate the safe delivery of these programmes.
- Usually, these groups of service users would have been physically brought together in a training room to attend the relevant programme and would have got to know each other. However, they still may not have shared email addresses or contact information.
- PBNI contacted all the service users, informed them of what had happened, requested them to delete the email and not to take note or use the information. A letter was also sent with the same information.
- PBNI have ensured that awareness of the need to carry out DPIAs has been raised with managers.
- On an ongoing basis throughout the Covid-19 pandemic staff were reminded of the data protection responsibilities in a variety of ways such as the Data Protection Officer recording a podcast and all staff memos.
- As the programmes were being delivered remotely the individuals selected for participation in the programmes were from different locations across Northern Ireland possibly making identification less likely.

- There is no evidence of damage or distress having been caused to the data subjects.

We also want to mention that PBNI has advised that its staff have undertaken extensive testing in relation to sending future emails to individual service user's email addresses to ensure that no other email addresses of others invited to attend the programme are shared. PBNI no longer sends a calendar WebEx invite but copies the WebEx link created as the invite for the meeting and sends the email from a separate PBNI account. PBNI is using the BCC function to email the link to participants and the subject line of the email says 'Link' and there is no other information contained in the body of the email other than the link to the WebEx event.

Whilst the investigation recognises that any clues to who the recipients are have been removed as much as possible from the emails it does not consider the use of BCC for group emails is secure enough considering the group of individuals who are involved and the risk of using CC inadvertently. This is an error the ICO has seen on many occasions. The numbers involved are relatively low in each programme so the ICO does not believe the sending of the link in individual emails should involve disproportionate effort.

However, after careful consideration and based on the information provided, we have decided to issue PBNI with a reprimand in accordance with Schedule 13(2) of the DPA 2018.

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed the DPA 2018:

- Section 40, the sixth data protection principle, which states that personal data must be processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures.
- Section 57 which states that a controller must implement technical and organisational measures into their processing activities from the design stage onwards.
- Section 64 which states that the controller must carry out a data protection impact assessment, if the processing is likely to result in a high risk to the rights and freedoms of individuals, to identify risks and minimise the data protection risks.

In particular, PBNI did not build in stringent and appropriate measures to provide security to the personal data (email addresses) of individuals attending these

programmes and did not identify the risks associated with delivering this service in a new way.

Further Action Recommended

The Commissioner recommends that PBNI could take certain steps to improve compliance with DPA 2018. In particular:

1. Introduce a more secure method of inviting service users to online programmes. This could be achieved by sending individual emails with the WebEx link or investigate a different approach. However, the ICO does not consider the use of BCC is a secure solution when sending group emails to this high risk group of individuals.
2. Review the content and frequency of your data protection and information security training to ensure that sufficient practical guidance is given to staff in how to comply with the data protection legislation. Consider your methods of monitoring and ensuring staff who deal with personal data complete this. In particular, refresher training should be provided, ideally annually, for all staff handling personal data.

3. Ensure the use of DPIAs in similar circumstances or when introducing a new service or way of delivery that involves handling personal data and consider consulting your Data Protection Officer on such matters.

For completeness, we ask that PBNI provides a progress update on steps 1 and 2 above in three months' time, or by no later than 19 August 2022. Please provide this update to [redacted]

Whilst the above measures are suggestions, I would like to point out that if further information relating to this subject comes to light, or if any further incidents or complaints are reported to us, we may revisit this matter and further formal regulatory action may be considered as a result.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link:

https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and new powers under the GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

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
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 United Kingdom 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 (https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

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 .

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