DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

The Information Commissioner (the Commissioner) issues a reprimand to The Patient and Client Council (PCC) in accordance with Article 58(2)(b) of the UK General Data Protection Regulation in respect of certain infringements of the UK GDPR.

On 20 January 2021 a member of PCC staff sent an email to 15 members of a Gender Identity Liaison Panel it was in the process of establishing. The panel was made up of individuals from across Northern Ireland who each had lived experience of gender dysphoria.

The email was sent to panel members in order to provide an update in respect of a delay in providing information; the body of the email did not contain any personal data. In error the recipient email addresses were carbon copied (CC) rather than blind carbon copied (BCC), thereby disclosing the email addresses of all panel members to each other. The incident was identified 03 February 2021 after one of the data subjects informed the Health and Social Care Board of the matter and complained.

Of the 15 email addresses disclosed 2 did not contain data sufficient to identify an individual however of the remaining 13 addresses, 10 were addresses containing a first name and surname and 3 were addresses containing initials and surname. It is considered that the 13 email addresses contained sufficient information to identify the data subjects.

Although the data contained in the email addresses was limited it is considered that the recipients of the email could reasonably infer that the other recipients also had experience of gender dysphoria given their inclusion as a recipient and therefore on the panel. As gender dysphoria is a medical condition it is considered that the data would constitute special category data, as per Article 9 of the UK GDPR.

Whilst the disclosure was limited to the 15 members of the panel, at the time of the disclosure it is understood that the panel had not yet convened and no evidence has been provided that the data subjects were already known to each other. In view of the sensitivity of the data it is considered that this is unlikely to be information the data subjects would want shared with individuals unknown to them and therefore the incident had the potential to cause distress to the affected data subjects.

The reprimand

The Commissioner has decided to issue a reprimand to PCC in respect of the following infringements of the UK GDPR:

- **Article 5 (1)(f)** which states the personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

- **Article 32 (1)** which states "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…"

The reasons for the Commissioner's findings are set out below.

Article 5 (1)(f)

Based on the findings of this investigation it is considered that the use of email and the BCC function was not a suitably secure method to communicate with the data subjects in this instance, given the sensitivity of the data, and that other more appropriate methods could have been used, such as sending individual emails to each data subject or purchasing a software package which ensured the secure sending of emails to recipients.

Whilst PCC did specify in its "PCC Use of Electronic Email Policy" that sensitive or patient data should not be emailed to addresses other than those from a specified list unless encrypted, the email involved in this incident was not encrypted, suggesting a potential lack of staff awareness of this requirement or a failure to implement this requirement in practice.

Article 32 (1)

It is also considered that PCC failed to provide sufficient policies, procedures or guidance which detailed for staff requirements when sending emails using the BCC function.

At the time of the incident whilst PCC had a number of policies in place, including its "PCC Use of Electronic Email Policy", none of the policies contained any guidance in respect of the use of BCC. It is also noted that the "PCC Use of Electronic Email Policy" in place at the time of the incident contained references to out of date legislation, i.e. the Data Protection Act 1998.

PCC has provided no evidence of any documented guidance materials in place, and accessible to staff, at the time of the incident providing information about the expected use of BCC and CC other than one slide within its Information Governance elearning training module which was limited in scope. PCC has stated that additional training framed the functionality of BCC and CC however no evidence documenting that this was in place prior to the incident has been provided.

Documented policies and guidance should have been in place at the time of the incident to ensure staff were sufficiently aware of what measures they should be implementing when communicating with individuals via email and BCC, particularly when involving special category data as in this instance. It is therefore considered that at the time of the incident there were insufficient documented policies or guidance which communicated PCC's expectations in respect of the use of BCC and CC when sending emails and that this contributed to the incident occurring.

Mitigating factors

In the course of our investigation we have noted that whilst the data disclosed was sensitive there is no evidence that the email addresses have been further used by any of the recipients.

Remedial steps taken by PCC

The Commissioner has also considered and welcomes the remedial steps taken by PCC in the light of this incident. In particular, upon becoming aware of the disclosure PCC contacted all recipients swiftly, requesting they delete the email, that they not use the email addresses disclosed and asking for confirmation this had been completed, which was received;

staff have been refreshed on relevant information governance, data protection policies and protocols to be adhered to; staff have been reminded about the appropriate use of email and the function of BCC and CC; staff have been engaged in individual and team meetings in relation to their roles and responsibilities within data protection, information governance and codes of conduct [redacted] PCC's Staff Agency day training on 07 March 2023 referenced BCC and PCC is undertaking a companywide review of policies with amendments to be made for which a timescale has not been provided.

Decision to issue a reprimand

Taking into account all the circumstances of this case, including the mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to PCC in relation to the alleged infringements of Article 5 (1)(f) and Article 32 (1) of the UK GDPR set out above.

Further Action Recommended

The Commissioner recommends that PCC should take certain steps to ensure its compliance with UK GDPR. With particular reference to Articles 5 (1)(f) and Article 32 (1) of the UK GDPR, the following steps are recommended:

1. In order to ensure compliance with Articles 5 (1)(f) and Article 32 (1) of the UK GDPR PCC should ensure that its policies, procedures and guidance are reviewed and updated so that appropriate guidance is provided to staff in respect of how and when to use the BCC function, in particular when sending emails to multiple recipients.

2. Take steps to communicate to staff the reviewed and updated policies, procedures and guidance in respect of BCC.

3. Consider undertaking an assessment, such as a Data Protection Impact Assessment (DPIA), to assess whether using email and the BCC function is a suitably appropriate communication method where special category data is included or can be inferred.

PCC should provide a progress update on the above recommendations within three months of the date of this reprimand, ie by 11 October 2023.