DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: Executive Office

OF: Castle Buildings
Stormont Estate
Belfast
BT4 3SR

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

In summary, on 22 May 2020 the Interim Advocate's Office (IAO) sent a newsletter by email to 251 subscribers on its mailing list. The email addresses of the recipients were visible to all who received the email.

The IAO was established following the findings and report of the Historical Institutional Abuse (HIA) Inquiry, which investigated abuse of children under 18 who were living in an institution in Northern Ireland between 1922 and 1995. One of the overarching recommendations made from the Inquiry was the appointment of a statutory Commissioner for Survivors of Institutional Childhood Abuse (COSICA). The Head of the Civil Service tasked the Executive Office officials to draft primary legislation predicated on the Inquiry recommendations for a COSICA. Separately, officials were tasked with appointing an Interim Advocate for victims and survivors of HIA, as a precursor to the appointment of the statutory Commissioner. The Interim Advocate was subsequently appointed on 2 July 2019 and the IAO was established on 12 August 2019.

At the time of reporting the breach the IAO described itself as an arm's length organisation, sponsored by but otherwise independent of, the Executive Office. However, on 11 December 2020 the IAO ceased to exist as the COSICA was established. Following this and subsequent legal advice, the Executive Office clarified that the IAO was a constituent part of the Executive Office with no separate legal basis. Therefore, the Executive Office is the relevant Data Controller in relation to data processed by the IAO

The reprimand

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

- **Article 5 (1)(f)** which states:

"*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 24 (1) and (2)** which states:

"1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.".

- **Article 32 (1) and (2)** which states:

"1. 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..".

"2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.".

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

- **Article 5 (1) (f)**:

The Commissioner considers that the IAO has failed to ensure appropriate security, resulting in the inappropriate disclosure of email addresses

relating to 209 individuals. Of those 209 email addresses, 110 email addresses contained the individuals' full name and the remainder of the email addresses contained a mixture of formulations of names, such as initials or first and last name only. It is noted that the individuals may not be identifiable from the email addresses alone, however the email addresses could be used to identify individuals in combination with other information.

The Commissioner considers that the IAO should have had a more secure process in place for the sending of group emails than inputting email addresses into the 'To' field and then copying them into the 'bcc' (blind carbon copy) field.

- **Article 24 (1) and (2)**:

The Commissioner considers that the IAO has failed to implement appropriate technical and organisational measures to ensure the security of personal data. There was no technical solution in place for the sending of group emails, such as mail merge. There was no documented process in place for the sending of the newsletter by group email and no training was provided to staff on the process.

Further to this, the IAO did not have appropriate data protection policies and procedures in place. The only data protection guidance available to staff was contained within an induction pack under the heading 'Procedures for Answering the Telephone'. The Commissioner considers that this guidance was inadequate in ensuring that staff were aware of their data protection responsibilities.

- **Article 32 (1) and (2)**:

The Commissioner considers that the IAO has failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks associated with the processing in this context. The IAO was working within a highly sensitive sector involving HIA and therefore confidentiality was of the utmost importance. The lack of appropriate measures indicates that the IAO did not have sufficient consideration of the security of personal data and the risks to the rights and freedoms of data subjects.

Mitigating factors

In the course of our investigation we have noted that the IAO took immediate steps to inform all of those affected and to update them on the investigation into the breach. The IAO also issued an apology to all of

those affected and put emotional support arrangements in place to help those affected.

Remedial steps taken by the IAO

The Commissioner has also considered and welcomes the remedial steps taken by the IAO following this incident. The IAO reviewed its process for sending the newsletter by group email and Newsletter Desk Instructions were created and issued to staff on 8 July 2020 to provide guidance on issuing the newsletter by group email.

A full review of the information management arrangements in place within the IAO was also carried out and on 1 July 2020, the Executive Office's Data Protection Officer took responsibility for the IAO. Data protection and information management policies and procedures were developed as a matter of urgency and existing policies and procedures were reviewed. As part of this review, the IAOs Data Protection Impact Assessment was reviewed and updated in July 2020, to clarify that the Executive Office was the relevant Data Controller.

Further to this, on 20 July 2020 the Executive Office circulated a report to the Northern Ireland Civil Service (NICS) Data Protection Officers' Forum to ensure lessons learned are shared across the wider NICS.

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 the Executive Office in relation to the infringements of **Article 5 (1)(f)**, **Article 24 (1) and (2)**, and **Article 32 (1) and (2)** of the UK GDPR as set out above.