Data Protection Report

Purpose

1. To provide a report, from a data protection perspective, to assist the assessment of a complaint about a Scottish Government member of staff.

Background

2. It is alleged that a [redacted] member of Scottish Government staff, breached various requirements of [redacted] by disclosing to a former employee, the name of one of the complainers under the Scottish Government's Procedure for the Handling of Harassment Complaints Involving Current or Former Ministers. This is alleged to have occurred during [redacted]. Both parties agree that the meeting took place at this time, but have provided differing accounts of what happened at that meeting.

3. It is further alleged that this disclosure was reported by the former member of staff to the Former First Minister and at least 3 other people.

4. As the data controller [1] for the information that is alleged to have been disclosed, Scottish Government has a responsibility for the lawful processing of that information. Given that the allegation is that this information was disclosed without authority to a party not entitled to receive it, Katrina Williams, Director General Scottish Government, commissioned Colin Cook, in his capacity as Deputy Senior Information Risk Owner Scottish Government, to assess the data protection issues potentially raised by this complaint. She also asked him to consider any further steps that might be taken to investigate the aspects of this complaint which relate to the Scottish Government's duties as data controller.

5. Colin Cook engaged [redacted] in preparing this report.

6. The focus of this work is on a potential breach of relevant data protection legislation. It does not therefore seek to offer an opinion on which of the accounts of the alleged incident is correct or consider any other potential issues relating to the [Redacted]

7. The incident being investigated took place on [redacted] 2018 and is therefore considered in terms of the Data Protection Act 1998.

8. Typically, an incident of this nature would be reported to the Information Assurance and Data Protection Branch of Scottish Government as a potential security incident by either the data subject [2] or the person responsible for the potential breach. The Branch would then work with the Data Protection Officer to assess whether it met the threshold to report to the Information Commissioner's Office. This judgement would be based on the sensitivity of the information concerned, the number of persons affected by its disclosure, the duration of the exposure and assessment of the potential impact on the rights and freedoms of the data subject. The data subject could also report the incident directly to the Information Commissioner's Office.

[1] References to "data controller" in this report are to the Scottish Minister/Scottish Government (SG)

[2] A "data subject" is a natural person - in this case, the person whose name was alleged to have been exchanged

ISO14001 at V.Q. BSI REGISTERED FS 31456 NATIONAL ACCREDITATION OF CERTIFICATION BODIES
INVESTORS IN PEOPLE | Accredited Until 2020
POSITIVE ABOUT DISABLED PEOPLE

9. In this instance, the allegation did not come to light until 2021 and was made by a former employee to a third party, Mr James Hamilton, during interviews relating to Mr Hamilton's independent report on the First Minister's self-referral under the Scottish Ministerial Code. Neither the data controller nor data subject were involved in this disclosure.

10. Scottish Government became aware of the allegation following the receipt of a letter to Permanent Secretary from Levy & Macrae on behalf of Mr Alex Salmond, dated 2nd March 2021 and the publication of Mr Hamilton's report. This is therefore the first opportunity that the Scottish Government has had to investigate the matter. [Redacted]

Issues Considered

11. The allegation is that a name was passed verbally in a meeting between [redacted] and a former Scottish Government employee. Both parties agree that this meeting took place, but no recording, documents or meeting records exist to confirm this.

12. There are two potential issues in this instance. First, the possibility that the individual who is alleged to have passed on this information has committed a data protection offence and second, the possibility that the data controller has breached data protection principles by failing to establish and operate the controls necessary to protect this information. In the first instance, any offence would have been committed by the person who passed on the information against the data controller. In the second instance, any potential offence would have been committed by the data controller against the data subject.

13. During this review, Scottish Government has confirmed that the Information Asset Owner did not give anybody permission to pass on the names of the complainants and that therefore if such a disclosure did take place, it would have happened without the consent of the data controller.

14. It is acknowledged that there are potentially other legitimate ways for the names of the complainants to have become known, such as through separate, but legitimate, connections between the individuals involved. The data controller is not party to any such mechanisms, but if they operated in this case, no data protection issues would arise for the controller.

Consideration

<u>The Actions of the Individual</u>

15. As stated above, the two individuals concerned agree that [redacted] but offer differing accounts of what was said at that meeting. These are covered in the report provided by Mr. James Hamilton and have been reviewed during this work. No recording, notes or other documents that might confirm either account have been discovered or offered in evidence at any stage in the proceedings.

16. As part of this consideration, Scottish Government has searched electronic records between [redacted] and has found no records relating to this meeting. Itemised mobile phone records are only available for the previous 12 months and so have not been considered, but given that

both parties agree that they met on [redacted] in [redacted] 2018, and that the incident in question is agreed to have been [redacted].

17. The individual who is alleged to have passed on the name is [redacted] and has not been specifically asked if they did so by a member of Scottish Government staff. However, that individual has already given an account to Mr Hamilton that they did not make this claim and also given a previous statement to the Data Protection Officer in August 2018 saying they had not passed on any related information to anyone who should not have it. In [redacted], the individual stated that they were not provided with the names of any complainant and so did not pass them on.

18. This report itself not does not seek to make a judgement on the content of the meeting in question, but proceeds on the basis that available, verbal evidence is contradictory and cannot be substantiated, at this stage by documentary evidence. Scottish Government staff or former staff have a right to privacy and an allegation of this nature, which could lead to dismissal or have implications for future employment, needs to be supported by a reasonable amount of evidence in order to take it forward.

19. In other cases where names of individuals have been released (not related to this case), these have been recorded as data protection incidents because staff have admitted a mistake and there is evidence of it happening. On the basis of the information available currently in this case however, there does not appear to be enough evidence to either record the incident internally as a data protection incident, or to report it externally to the Information Commissioner's Office.

Scottish Duties as Data Controller

20. To date, the data subject whose name was allegedly disclosed has not made a complaint about the Scottish Government in respect of this matter. Privacy rights lie with data subjects. A third party cannot complain to the Information Commissioner's Office on behalf of another without that data subject's agreement to act on their behalf.

21. A letter to the Permanent Secretary from Levy & Macrae on behalf of Mr Salmond, dated 2nd March 2021, states that the alleged disclosure contravenes previous assurances given by the Permanent Secretary that the Scottish Government was handling the "process with the utmost care and commitment to confidentiality".

22. As part of this investigation, consideration has therefore been given to whether Scottish Government had appropriate technical and organisational controls in place to protect personal information and whether staff operated in accordance with these controls.

23. Appropriate data handling policies and procedures were in place at the time of the alleged disclosure. Copies of the relevant polices; the "SG Information Security Policy Statement" "SG Data Handling Policy" and "SG Data Protection Policy" are attached to this email. All of these were updated April 2015 and not renewed again until after the date of the alleged incident.

24. HR policy at that time, was that a transgression of these policies by a staff member would be looked at as a disciplinary breach as detailed in the Scottish Government Staff Handbook.

25. Data Protection Training was available to Scottish Government staff. The staff member had undertaken data protection training and was up to date with that training at the time of the incident.

26. Cyber checks looking at access to information on eRDM, local drives and e-mail traffic for information relating to the issues relating to complaints against the Former First Minister were undertaken in 2018 and again in 2020 using NUIX, a world leading technology for these forms of investigative exercises. These searches found no suspicious traffic or mishandling of information.

27. Whilst the events of [redacted] 2018 were not considered specifically at the time of these extensive searches, consideration was given to general data handling of material relating to the case and the specific actions of people with access to the information that is alleged to have been passed on. This showed that appropriate processes were in place, and followed, and that no person was identified as having breached these processes. This was also the conclusion of the Information Commissioner's Office. The Information Commissioners Office conducted its own review of the investigation and did not change that view.

28. The handling of the relevant data during the period of the allegation therefore appears to have been sound. Consequently, it was appropriate for Scottish Government to give assurances on this to Committee. The information was handled securely from the end of 2017 up to the point of being obtained by the press in August 2018 by means unknown.

Further Action

29. Scottish Government takes its responsibilities for data protection extremely seriously. In this case however, the absence of evidence to corroborate the allegation that an offence has taken place, suggests that no further action should be taken at this stage. If the evidence base changes, for example through the recovery of an email or document relating to the meeting or the testimony from an individual admits to a mistake, or if Scottish Government were to receive a complaint from the data subject that can be evidenced or corroborated, this position would be reviewed immediately.

30. [redacted]

31. Further action in respect of these allegations can be instigated by either the data subject or the data controller, as they are the parties that can be offended against. This requires the data controller or subject to inform the Information Commissioner's Office or the Police, depending on the nature of the offence. The Information Commissioner's Office would typically expect that the data subject is able to show that the data controller has already attempted to explain or resolve an issue before proceeding with this course of action.

32. In theory, anybody, at any time, can commence legal action, but without the involvement of the Police or the Information Commissioner's Office, these are unlikely to succeed without prior engagement between data subject and controller.

33. Given the information presented above, we recommend that no further action is taken at this stage in respect of the alleged data protection breach. This decision should however be revisited if new evidence emerges or there is any other material change in circumstances. The

ISO14001 at V.Q.
INVESTORS IN PEOPLE | Accredited Until 2020

applicable regulations that would be engaged should more information come to light are set out in Annex A of this document.

Authors

Colin Cook, Director Digital, Deputy SIRO
[Redacted]