

Decision Notice

Decision 21/2024: Information and Digital Technologies Department

Consultant records

Reference no: 2021023

Decision date: 26 July 2024

Summary

The Applicant made a request under the Public Access to Information (**PATI**) Act 2010 to the Information and Digital Technologies Department (**Department**) for records relating to a specific consultancy contract. The Department granted access to twelve responsive records but denied access to the remaining records under sections 30(1)(b) (operations of public authorities) and 32(1)(a) (national security). The Department also refused part of the PATI request under section 16(1)(f), because the information being sought was available in the public domain. The Applicant challenged the Department's refusal as well as the reasonableness of its search to locate the records responsive to the PATI request.

During the Information Commissioner's review, the Applicant agreed to narrow the scope of their challenge of the Department's internal review decision, which resulted in the removal of certain parts of the records. These parts have been considered non-responsive.

The Information Commissioner has found that the Department did not conduct a reasonable search to locate records responsive to a specific part of the PATI request. The Department was further not justified on relying on the administrative denial in section 16(1)(f). Lastly, the Information Commissioner has found that the Department was not justified in relying on the exemptions in sections 30(1)(b) and 32(1)(a) to deny access to the parts of the withheld records still at issue. On her own accord, the Information Commissioner found that certain parts in the records were exempt under the personal information exemption in section 23(1).

Relevant statutory provisions

Public Access to Information Act 2010: section 12(2)(b) (completeness/accuracy of response), section 16(1)(f) (administrative denial: already in public domain), section 21 (public interest test), section 23(1) (personal information), section 24 (definition of personal information), section 30(1)(b) (operations of public authorities: management functions), section 32(1)(a) (national security, defence, and international relations: security, defence or relations).

Public Access to Information Regulations 2014: regulation 5 (reasonable search).

Appendix I provides the text of these statutory provisions and forms part of this Decision.

Background

1. On 1 April 2021, the Information and Digital Technologies Department (**Department**) entered into a service agreement for research services with Info-Tech. Based on the

information published in the Official Gazette Notice, the service agreement was originally signed for a period of one year¹ but later extended to 31 March 2024.²

2. On 21 June 2022, the Department requested a single-source waiver³ from the Office of Project Management and Procurement (**OPMP**) for a 3-month contract with Info-Tech to provide the Department with a Chief Information Security Officer (**CISO**).⁴ It is unclear whether the waiver was obtained from the Director of OPMP or if the contract was actually executed.
3. On or around 10 August 2022, the Department entered into a service agreement with Cyberdine⁵ for a Virtual Chief Information Security Officer (**VCISO**) service.⁶
4. On 4 February 2023, the Applicant made a request under the Public Access to Information (**PATI**) Act 2010 to the Information Commissioner's Office (**ICO**) asking for the following records from between 1 August 2022 and 5 February 2023:
 - a. A copy of the contract or statement of work for Cyberdine security consultant, including information on the amount and length of the contract and extension (**item 1a**),⁷ items delivered or completed during the original contract (**item 1b**) and rationale for extension (**item 1c**).
 - b. Invoices sent from Cyberdine to any Government department (**item 2**).
 - c. Payments sent from any Government department to Cyberdine (**item 3**).

¹ See [GN1440/2021](#) published on 28 December 2021. According to this Gazette Notice, the agreement with Info-Tech was to end on 1 April 2022.

² According to [GN1175/2022](#) published on 31 December 2022, the agreement with Info-Tech was to end on 1 April 2023. [GN0513/2024](#) published on 21 May 2024 shows that the agreement ended on 31 March 2024.

³ Under paragraph 24.4 of the [Code of Practice for Project Management and Procurement](#), public officers may engage in single-source or non-competitive procurement only where the Director of the Office of Project Management and Procurement (**OPMP**) determines that any of the following exceptional circumstances applies: the subject matter of the procurement is available only from a particular supplier or contractor, an extreme need owing to a catastrophic event, the single-source procurement is needed due to standardisation or compatibility reasons, and the use of any other method of procurement is not appropriate for the protection of essential security interests of Bermuda.

⁴ Based on an email sent by the Department to the OPMP on 21 June 2022, which was disclosed by the OPMP in response to a separate PATI request.

⁵ Also referred to as Cyberdyne at times.

⁶ Gazette Notice [GN1175/2022](#), published on 13 December 2022.

⁷ The PATI request itself included the contract extension as a separate sub-item, however, the contract amount, length and extensions have been combined in this Decision for ease of reference.

5. On 7 February 2023, the ICO transferred the PATI request in full to the Department.
6. After it extended the timeline to issue an initial decision, on 2 May 2023, the Department issued an initial decision informing the Applicant that some of the responsive records were exempt under sections 30(1)(b) (management functions) and 32(1)(a) (national security). Although the initial decision informed the Applicant that access to some of the responsive records would be granted, the Department did not immediately disclose the records to give Cyberdine (as an interested third party) an opportunity to seek an internal review.
7. On 15 June 2023, the Applicant asked for an internal review.
8. On 20 June 2023, the Department informed the Applicant that Cyberdine did not ask for an internal review. The Department also disclosed a number of emails (some of which were redacted) and invoices responsive to the PATI request. Later during the Information Commissioner's review, the Applicant confirmed that the disclosed invoices satisfied items 2 and 3 of the PATI request and they did not wish to challenge the redactions in the disclosed emails or to obtain access to the cover emails attaching the Status Reports from Cyberdine to the Department updating the Chief Information Office (**CIO**) on Cyberdine's activity progress (**Status Reports**).
9. On 1 August 2023, the Department issued an internal review decision, affirming the denial of access to records responsive to items 1b and 1c under the exemptions in sections 30(1)(b) and 32(1)(a). The Department administratively denied access to parts of the records responsive to item 1a under section 16(1)(f), because it believed that the relevant information was available in the public domain.
10. On 1 August 2023, the Applicant asked for an independent review by the Information Commissioner, to challenge the Department's internal review decision.

Investigation

11. The ICO accepted the application as valid on 9 August 2023, on the basis that the Applicant had made a PATI request to a public authority and had asked that public authority for an internal review. The ICO also confirmed the issues the Applicant wanted the Information Commissioner to review.
12. The Information Commissioner decided that early resolution under section 46 of the PATI Act was not appropriate for this application, because submissions from the public authority were required on the exemptions, administrative denial and the reasonableness of the Department's search.

13. The ICO notified the Department of the valid application on 10 August 2023 and asked for the withheld responsive records. Throughout the review, the Department submitted a number of records, including those now considered in this Decision: two service agreements (**records 1 and 2**) responsive to item 1a and nine weekly Status Reports (**records 3, 4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11**)⁸ responsive to item 1b.⁹ The Department did not provide any records responsive to item 1c.
14. As required by section 47(4) of the PATI Act, the Department and the Applicant were invited to make representations to the Information Commissioner. Because the records involved Cyberdine and a Cyberdine employee, they were identified as a collective concerned third party (**Third Party**) and were also invited to make representations to the Information Commissioner. On 23 January 2024, the Applicant responded to the formal invitation to make submissions and provided additional information throughout the review. On 18 March 2024, the Department made formal submissions on section 16(1)(f) and the exemptions.
15. During the review, the Applicant confirmed that they no longer challenged the Department's refusal to disclose information in the withheld records which could identify the actual deliverables. The Applicant instead wished to challenge the reasonableness of the Department's search and its decision to withhold other information (apart from the actual deliverables) in records 1 and 2, as well as any information showing the progress or status of the deliverables in records 3, 4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11. Given this, and with the Applicant's agreement, the redactions of certain parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 which could identify the actual deliverables were removed from the review and are not considered in this Decision.
16. On 8 May 2024, the Department was invited to make submissions on the reasonableness of its search, particularly with regard to records responsive to item 1c of the PATI request seeking the rationale for the contract extension. The Department did not make submissions on the search issue.
17. The Third Party did not make a written submission to the ICO to object to the disclosure of the responsive parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 based on their third-party interests protected under sections 23, 25 and 26 of the PATI Act. Instead, the Third Party submitted proposed redactions to records 1 and 2 to the Department based

⁸ Records 5, 6, 7, 8 and 9 were the cover emails attaching the Status Reports which the Applicant is no longer interested in pursuing (see paragraph 8 above). These emails are no longer considered in this review. Records 5.1, 6.1, 7.1, 8.1 and 9.1 were the weekly Status Reports attached to those emails.

⁹ As explained in paragraph 15, this Decision only considered the parts of these records that are still at issue.

on other provisions of the PATI Act. In turn, the Department asserted its reliance on these redactions in this review and the Information Commissioner considered these submissions from the Department. At the end of June and in early July 2024, the Third Party suggested that it might make a submission, though the submission would depend on additional information it had requested from the Department. The ICO reiterated the specific rights the PATI Act affords to a third party and emphasised that the Third Party had received copies of all relevant records for the purposes of making a submission. The ICO provided the Third Party with additional time to make submissions. The Third Party did not make a submission.

Information Commissioner's analysis and findings

18. The Information Commissioner has considered all relevant submissions, or parts of submissions, made by the parties. She is satisfied that no matter of relevance has been overlooked.
19. The Information Commissioner strives to provide as full a public explanation of her reasoning and Decision as possible. Section 53(2) of the PATI Act, however, prevents discussion of the withheld records. As a result, the analysis below cannot be as detailed as would otherwise be preferred.

Reasonable search – section 12(2)(b) of the PATI Act and regulation 5 of the PATI Regulations

20. Section 12(2)(b) of the PATI Act requires public authorities to make every reasonable effort to respond to PATI requests completely and accurately. Regulation 5 of the PATI Regulations requires public authorities, through their Information Officers, to make reasonable efforts to locate records responsive to a PATI request. Regulation 5(2) requires a public authority to document its efforts if it has been unable to locate any record. Read together, these provisions require public authorities to conduct a reasonable search in response to a PATI request.
21. In cases where the reasonableness of a public authority's search is in question, the Information Commissioner's task is to assess whether such search was reasonable in accordance with the provisions of the PATI Act and Regulations. It is not her role to assess whether a public authority should or should not hold a record as a matter of good public administration.
22. In determining whether a public authority's search was reasonable, the Information Commissioner takes into account the following:

[1] the quality of the public authority's analysis of the PATI request;

- [2] the scope of the search that it decided to make on the basis of that analysis; and
- [3] the rigour and efficiency with which the search was then conducted.

23. The specific circumstances in each case will inform the Information Commissioner's assessment.
24. Finally, the public authority bears the burden to establish, on the balance of probabilities, that responsive records did not exist or could not be found after all reasonable steps were taken to find them.¹⁰

Public authority's submissions

25. The Department did not make any submission on the reasonableness of its search to locate records responsive to item 1c of the PATI request or to locate the records responsive to all of item 1.

Applicant's submissions

26. The Applicant explained that item 1c asked for records explaining the reasons for the Department's decision to extend the service agreement with Cyberdine. They also explained that, in accordance with paragraph 38.1(a) of the [Code of Practice for Project Management and Procurement \(Procurement Code of Practice\)](#), the extension of a contract with a value of less than \$100,000 must be approved in writing by the CIO as the Accounting Officer for the Department.¹¹ The Applicant submitted that the written approval for extending Cyberdine's contract "would likely" have the rationale for the extensions. The Applicant submitted that they explained the scope of item 1c to the Department during its initial handling of the PATI request. The Applicant submitted their correspondence with the Department to support their assertion.
27. More generally, the Applicant submitted that their PATI request should have been understood to be asking for records relating to both Cyberdine and Info-Tech. The Applicant explained their reasons, including the fact that the PATI request included

¹⁰ See [Decision 04/2017, Department of Health](#), at paragraphs 37-49, and more recently [Decision 17/2024, Ministry of National Security Headquarters](#), at paragraphs 18-37.

¹¹ The relevant paragraph, under 'Contract Variation and Extension' of the Code of Practice reads: "38.1 The term of a contract must be stated and not be extended beyond the period for which the contract was awarded unless the original contract provides for an extension of the contract term, or the contract term is extended by a written amendment to the contract. (a) An extension of the term of a contract with a value of less than \$100,000 must be authorised in writing by the Accounting Officer. The Accounting Officer may only approve an extension if the Accounting Officer determines that the extension will achieve Best Value for the Government and complies with all legal requirements."

'infotech' as one of the suggested search keywords. The Applicant also submitted a record obtained from a PATI request made to another public authority which shows that the Department's CIO requested a waiver for a 3-month contract for Info-Tech to provide the Department with a CISO.

Discussion

28. The reasonableness of the Department's search is at issue because the Applicant challenged the fact that the Department did not identify (a) any records which confirmed the Department's compliance with paragraph 38.1(a) of the Procurement Code of Practice that would have been responsive to item 1c, and (b) certain records related to Info-Tech. These two matters are considered separately.

[1] The quality of the public authority's analysis of the PATI request

29. The PATI request asked for:

"1. Copy of contract/statement of work for Cyberdine (Cyberdyne) Security Consultant [name redacted] (from [the Attorney General's] Chambers)

- Amount/length of original contract
- Items delivered/completed during original contract
- Rationale for extension
- Cost/length of extension(s)

...

Date would range between 1 August 2022 and 5 February 2023

Helpful search terms would be: Cyberdine, Cyberdyne, infotech, [Cyberdine employee's names], CISO, VCISO"

Rationale for extension (item 1c)

30. Item 1c asked for the Department's rationale for extending its service agreement with Cyberdine. While the PATI request itself did not specifically refer to the Procurement Code of Practice, further correspondence from the Applicant (including their email to the Department of 30 March 2023 and their internal review request) made it clear that the PATI request should be understood in the context of the procurement process. Based on this, and in the absence of submissions on this point from the Department, the Information Commissioner is not satisfied that the Department's analysis of item 1c of

the request was adequate. The Information Commissioner consequently concludes that the Department's search for this specific part of the PATI request was not reasonable. The reasonableness of the Department's search for this part of the request is not considered further.

Certain records on Info-Tech (items 1a, 1b and 1c)

31. In contrast, the Information Commissioner is satisfied that the Department's reading of the PATI request as asking for records relating to Cyberdine only (thus excluding any records relating to Info-Tech) was adequate. While the PATI request did suggest "infotech" as one of the search keywords, it also specifically asked for records from 1 August 2022 to 5 February 2023. Based on this specific timeline, it was reasonable for the Department to limit the scope of the PATI request to be asking for records relating to Cyberdine only.

[2] The scope of the search that it decided to make based on that analysis

32. The Department did not make a submission on this point, but the records it retrieved and identified as responsive to the PATI request showed that the Department contacted the CIO and searched the CIO's emails to locate the responsive Cyberdine records. The Information Commissioner is satisfied that the scope of the Department's search was adequate based on its understanding of the PATI request above.

[3] The rigour and efficiency with which the search was then conducted

33. The search for responsive records was conducted by an officer within the Department who had sufficient knowledge on the subject and who had full access to the relevant locations of the records. Where there were gaps in the Status Reports identified by the ICO, the Department provided additional records during the review. The Information Commissioner is satisfied that the search was conducted with adequate rigour and efficiency.

Conclusion

34. The Department did not conduct a reasonable search to locate the records responsive to item 1c of the PATI request, but did so for the remainder of the request in accordance with section 12(2)(b) of the PATI Act and regulation 5 of the PATI Regulations.

Information in public domain – section 16(1)(f)

35. Section 16(1)(f) allows public authorities to refuse a PATI request under three specific circumstances, when the information sought is:

- a. in the public domain;
 - b. reasonably accessible to the public; or
 - c. reasonably available to the public on request under any other statutory provision, whether free of charge or on payment.
36. Here, under consideration is the assertion that the information in the responsive record is already in the public domain. This includes information that is publicly available on the internet. Section 16(1)(f) is not applicable, however, if it is not evident that all information in the responsive record is publicly available.
37. To administratively deny a PATI request under section 16(1)(f), a public authority must consider the following:
- [1] What information is in the record which falls within the PATI request?
 - [2] Is the information available in the public domain, including on the internet?
38. A public authority also has a duty to assist a requester in connection with a PATI request under section 12(2)(a). Under this duty, when a public authority relies on section 16(1)(f) to administratively deny a request, the public authority should provide the requester with details on how to access the public information.
39. Finally, the public authority bears the burden to establish, on the balance of probabilities, that it was justified to administratively deny the PATI request.¹²

Public authority's submissions

40. The Department explained in its internal review decision that the amounts and lengths of the original service agreement and extension were already in the public domain.

Applicant's submissions

41. The Applicant accepted that some information about Cyberdine service agreements was published in the Official Gazette Notice [GN1175/2022 \(2022 Gazette Notice\)](#). But the Applicant pointed out that the information in the [2022 Gazette Notice](#) did not identify the length of the original service agreement and instead reported 10 August 2022 to 31 January 2023 as the period of the service agreement.
42. In response to a Parliamentary question on 19 May 2023, the Premier/Minister of Finance announced the value of a Cyberdine service agreement from 16 February to 15

¹² See [Decision 17/2019, Ministry of Finance Headquarters](#), at paragraphs 15-19.

June 2023. The Applicant pointed out that, because the [2022 Gazette Notice](#) covered the period from 10 August 2022 to 31 January 2023 only, there was an unexplained 15-day gap from 1 to 15 February 2023.

43. The Applicant submitted that the value of the service agreements included in the [2022 Gazette Notice](#) was inaccurate. The Applicant provided relevant documents to support this assertion. As a result, the Applicant submitted that parts of records 1 and 2 were not properly denied under section 16(1)(f) because the requested information was not publicly available.

Discussion

44. The Department's reliance on section 16(1)(f) is considered for its decision to administratively deny public access to relevant parts of records 1 and 2.

[1] What information is in the record which falls within the PATI request?

45. Having reviewed the relevant parts in records 1 and 2, the Information Commissioner is satisfied that they contained information that is responsive to item 1a of the PATI request, namely, the amounts and lengths of the original Cyberdine service agreement and extension.

[2] Is the information available in the public domain, including on the internet?

46. The Department's internal review decision did not refer to the exact location in the public domain which contained the relevant information. However, based on the Applicant's submission and an internet search, it was likely that the Department was referring to the [2022 Gazette Notice](#) and the House of Assembly's [Official Hansard Report](#) of 19 May 2023 as the locations in which the responsive information could be found.
47. Because the service agreement period mentioned in the Premier/Minister of Finance's statement in the House of Assembly was outside the period responsive to the PATI request, the Information Commissioner is satisfied that the [Official Hansard Report](#) did not contain the same information on the amounts and lengths of the service agreements captured in records 1 and 2.
48. Having compared the information published in the [2022 Gazette Notice](#) and the relevant information in records 1 and 2, the Information Commissioner is satisfied that the [2022 Gazette Notice](#) summarised the combined amounts and lengths of the original service agreement and extension captured in the two records. But the Information Commissioner agrees with the Applicant that the relevant information shown in these records was not the same information published in the [2022 Gazette Notice](#). There was

information in the records that was not captured in the [2022 Gazette Notice](#). Based on this, the Information Commissioner is not satisfied that the Department's reliance on section 16(1)(f) to withhold information about the amounts and lengths of the original service agreement and extension in records 1 and 2 was justified.

49. It is noted that, on 21 May 2024 while the Information Commissioner's review was ongoing, the Department published Gazette Notice [GN0513/2024 \(2024 Gazette Notice\)](#) which contained further information about its service agreements with Cyberdine. Because the [2024 Gazette Notice](#) was published after the Department's internal review decision, the Information Commissioner did not take it into account in considering the Department's reliance on section 16(1)(f). Even if she did, she would have remained unsatisfied that the Department's reliance on the administrative denial was justified, on the basis that the [2024 Gazette Notice](#) also did not contain the same information captured in withheld records 1 and 2.

Conclusion

50. The Department was not justified in relying on section 16(1)(f) to administratively deny public access to certain parts of records 1 and 2.

National security – section 32(1)(a)

51. A record is exempt under section 32(1)(a) of the PATI Act if its disclosure would prejudice, or could reasonably be expected to prejudice, Bermuda's security or defence or its relations with any State or international organisation of States. In this case, the Department invoked the exemption as it believed that the records could prejudice Bermuda's security.
52. 'Prejudice' means a harm that is actual, real and significant.
53. To appropriately rely on section 32(1)(a), a public authority must consider the following:
- [1] What is the relevant prejudice, either to the security and/or defence of Bermuda and/or relations between Bermuda and any State or international organisation of States?
 - [2] What is the likelihood of the prejudice occurring?
 - [3] If the exemption is engaged, does the balance of the public interest require disclosure?
54. A public authority invoking section 32(1)(a) has the burden to show that, on the balance of probabilities, the exemption is justified.

Public authority's submissions

55. The Department submitted that disclosure of the records would impair its ability to manage unlawful access, theft and vandalism to its systems as well as to safeguard the data held in those systems. Disclosure would likely put the Government at an increased risk of being targeted by cybercriminals as it would reveal the specific IT systems or software used. Cybercriminals would then be able to use the information known about the specific systems, software, hardware, contracts or deliverables to target known vulnerabilities and gain unlawful access to information held by the Government. This would in turn damage the Government's financial, contractual, reputational and legal compliance requirements. Once a weakness that the contractor is engaged to fix is disclosed, the attackers would have a roadmap to attack the Government's IT infrastructure.
56. The Department considered that the release and subsequent harm or damage would or would likely occur if the records were disclosed. The Department emphasised that "would" means that, on balance, the disclosure would be more probable (greater than 50%) than not to lead to prejudice. "Would likely" means that, on balance, there is a real and significant risk of prejudice occurring even though the probability might be less than 50%.
57. The Department accepted that there is a public interest in promoting transparency, accountability, public understanding and involvement in the democratic process and in fully understanding the reasons for public authorities' decisions. However, disclosure would make the Government vulnerable to cybercrime as it outlines the Government's security position which could be used as a starting point to attack network infrastructure and/or information system.

Applicant's submissions

58. The Applicant submitted that they understand some of the risk involved in revealing too much information about the deliverables. Although the Applicant maintained that some of the descriptions of the deliverables might not be specific enough to threaten the security of the Government's IT system, they agreed to accept redactions of any information that would identify the deliverables.
59. The Applicant continued to want to obtain access to information on the status and/or number of items delivered in the responsive records because they believed that disclosure of the same was in the public interest. In their submissions throughout the review, the Applicant highlighted the importance of public authorities' compliance with the Procurement Code of Practice and the Government's Financial Instructions during

the procurement process. The Applicant emphasised public authorities' responsibility to prioritise merit and value for money when using public funds for contracting services.

60. The Applicant also emphasised the high value of the Cyberdine service agreements. The Applicant highlighted that based on information in the [2022 Gazette Notice](#) and the Premier's statement, the total value of these service agreements from 10 August 2022 to 15 June 2023 alone amounted to \$274,000. Given the Department has published a Request for Proposal for IT Research and Advisory Services during the Information Commissioner's review, the Applicant suspected that it would further extend Cyberdine's service agreement. The Applicant claimed that the length of Cyberdine's service agreement is now much longer than what was originally planned.
61. The Applicant emphasised that, under the Procurement Code of Practice, all single-source procurement above \$100,000 and all procurements with a value of at least \$250,000 must be approved by Cabinet. The Applicant queried the Department's compliance with the relevant provisions of the Procurement Code of Practice and whether the service agreements were awarded with adequate due diligence. The Applicant further questioned the value for money of the service agreement and extensions and emphasised that a decision to award and renew service agreements should be based on merit.
62. The Applicant submitted other information and various documents, including records related to the Department's procurement services from Info-Tech, which they received in response to a PATI request made to another public authority.

Discussion

63. As explained in paragraph 15, certain parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 which identified the actual deliverables were removed from the review. The Department continued to maintain that section 32(1)(a) justified withholding the remainder of the records. Accordingly, the Information Commissioner considers the Department's reliance on the exemption only for the remainder parts of these records.

[1] What was the relevant prejudice, either to the security and/or defence of Bermuda and/or relations between Bermuda and any State or international organisation of States?

64. The Government's IT system protects a wide range of information, including sensitive information which, if accessed by unauthorised parties, could reasonably harm Bermuda's security. The Information Commissioner accepts that an increased risk of a cybersecurity attack on the Government's IT system amounted to prejudice to Bermuda's security.

[2] What was the likelihood of the prejudice occurring?

65. After information which could identify the deliverables was removed, it is unclear how disclosure of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 could have reasonably been expected to result in an increased risk of a cybersecurity attack on the Government's IT system.
66. Once the Objectives and Deliverables in Appendix 1 in records 1 and 2 were removed, all that was left in the records were the dates of the Service Agreements, details of the parties as well as standardised general terms and conditions which could be found in most, if not all, the Government of Bermuda's vendor service agreements. The descriptions and overview of the service provided by Cyberdine were very generic and did not include any information which could reveal the specific IT systems or software used by the Government, or areas of vulnerability within the system.
67. Similarly, once the information identifying the deliverables was removed from records 3, 4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11, all that was left in these records was the cover pages of the Status Reports and information on relevant reporting periods, the owners and status of specific projects or activities as well as their completion targets, none of which identified the deliverables. None of this information included any details which could reveal the specific IT systems or software used by the Government, or any other information, which could in turn allow cybercriminals to target the system vulnerabilities to gain unlawful access to information, as claimed by the Department.

Conclusion

68. The Department was not justified in relying on section 32(1)(a) to withhold the remainder of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11.

Management functions – section 30(1)(b)

69. A public authority may rely on section 30(1)(b) to deny access to a public record whose disclosure could reasonably be expected to have a significant, adverse effect on a public authority's performance of any of its functions relating to management.
70. A public authority must identify the relevant management function involved. Further, it must show how disclosure could reasonably be expected to cause the specific harm, i.e. a significant, adverse effect on the performance of any management function.¹³

¹³ See the [ICO Guidance: operations of public authorities \(section 30\)](#) (October 2023).

71. Section 30(1)(b) refers to two examples of the relevant functions, namely a public authority's industrial relations and management of its staff. Generally, 'management functions' relate to a public authority's internal management of its routine operations. They may include strategic planning, financial resource management, security of IT functions, complaints handling and operational assessments (for instance, reviewing existing processes, proposing new ones and piloting them). Management functions should be understood as a narrower category of activity than a public authority's performance of its statutory functions that are assigned to it in law.
72. 'Having a significant, adverse effect' is not defined in the PATI Act.¹⁴ By its ordinary definition, it means bringing about an unfavourable or harmful result whose damage is severe, which is a stronger showing of harm than the usual standard of 'prejudice'.
73. Further, the likelihood must be that a reasonable person may expect the anticipated harm to occur considering all circumstances of the case. The expectations have to be likely, plausible or possible based on real and substantial factual grounds.
74. If section 30(1)(b) is properly engaged, the public interest test must be applied. Where the public interest would, on balance, be better served by disclosure than by non-disclosure, then the records must still be disclosed.
75. In sum, when applying the exemption in section 30(1)(b), a public authority must ask:
 - [1] What is the relevant function relating to management of the public authority?
 - [2] What is the specific significant, adverse effect?
 - [3] How could disclosure cause the significant, adverse effect on the identified management function?
 - [4] What is the likelihood of the significant, adverse effect occurring?
 - [5] If the exemption is engaged, does the balance of the public interest require disclosure?
76. A public authority bears the burden of satisfying the Information Commissioner that, on the balance of probabilities, it has provided sufficient support to justify its reliance on section 30(1)(b) to deny access to the records.

¹⁴ This harm standard is different from 'prejudice', which applies to most other exemptions in the PATI Act. It may be understood in the same terms as the harm standard for section 31(1), i.e., having a 'serious adverse effect'.

Public authority's submissions

77. The Department relied on the same arguments described in paragraphs 55-57.

Applicant's submissions

78. The Applicant argued that disclosure and transparency would assist with the Department's management functions.
79. The Applicant relied on the same arguments described in paragraphs 58-62.

Discussion

80. As explained in paragraph 15, certain parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 which could identify the actual deliverables were removed from the review. Because the Department made its submission on section 30(1)(b) after these parts of records were removed from the review, the Information Commissioner considers the Department's reliance on the exemption for the remainder parts of these records only.

[1] What was the relevant function relating to management of the public authority?

81. The Information Commissioner accepts that the Department's function to manage unlawful access, theft and vandalism to its IT system and safeguard the data held in those systems was a function relating to management. Unlike most Government departments, the Department does not have a statutory function. It was instead established to provide services internal to the Government.

[2] What was the specific significant, adverse effect?

82. The Information Commissioner further accepts that an increased risk of a cybersecurity attack on the Government IT system would amount to a significant, adverse effect. As shown by the attack on the Government IT system in September 2023, an attack on the Government IT system would have a serious negative effect on the quality of the public service.

[3] How could disclosure cause the significant, adverse effect on the identified management function?

83. As explained above, once information identifying the deliverables was removed, records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 contained generic information only. Given this and because the Department has not provided sufficient submissions on how disclosure of the responsive parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 could reasonably have resulted in the identified significant adverse effect, the Information Commissioner

is not satisfied that the Department's reliance on section 30(1)(b) was justified. She does not consider the Department's reliance on the exemption further.

Conclusion

84. The Department was not justified in relying on section 30(1)(b) to withhold the remainder of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11.

Personal information – section 23(1)

85. Under section 23(1) of the PATI Act, public authorities may deny public access to records or parts of records which consist of personal information. Section 24(1) broadly defines 'personal information' as information recorded in any form about an identifiable individual.
86. Certain information about identifiable individuals is excluded from the definition of 'personal information' in the PATI Act, in accordance with section 24(2). For example, section 24(2) excludes certain information about contractors performing services for a public authority.
87. The exemption in section 23(1) also does not apply to the limited circumstances set out in subsection (2), none of which are applicable here.
88. The personal information exemption is subject to the public interest test. Records which are found to be exempt under section 23(1) would still have to be disclosed, if the public interest would, on balance, be better served by disclosure instead of non-disclosure. In considering the public interest test for disclosure of personal information, the following factors have to be taken into consideration:¹⁵
- a. Whether disclosure will further the public interest, including but not limited to the factors listed in regulation 2 of the PATI Regulations.
 - b. Whether disclosure would be fair to the individual under all of the circumstances. Evaluating the fairness of any disclosure may include consideration of the following:
 - i. Whether sensitive personal information was involved?
 - ii. What would be the consequences upon the individual of disclosure?
 - iii. What are the reasonable expectations of privacy of a person in the individual's position?

¹⁵ [Decision 02/2019](#), Office of the Governor, paragraph 51.

c. Whether disclosure of the personal information is necessary to further the public interests that have been identified.

89. In sum, as the Information Commissioner explained in [Decision 02/2019, Office of the Governor](#), public authorities must consider the following questions before denying public access to records under the personal information exemption:¹⁶

[1] Whether the records consisted of information about an identifiable individual?

[2] Whether the information fell within any of the exclusions to the definition of personal information (section 24(2))?

[3] Whether any of the exceptions to the exemption in section 23(2) applied to the records?

[4] If the exemption for personal information in section 23(1) was engaged, whether the balance of the public interest required disclosure?

90. Given the importance of the protection of personal information and privacy, particularly in a small jurisdiction such as Bermuda, the Information Commissioner may consider the personal information exemption on her own accord and without the provision being relied upon by any of the parties, as she does in this review.

Discussion

[1] Whether the records consisted of information about an identifiable individual?

91. Certain parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 contained information about identifiable individuals, namely, employees of Cyberdine and the Department, including the Department's CIO.

[2] Whether the information fell within any of the exclusions to the definition of personal information (section 24(2))?

92. Although the CIO and the Department's staff were officers or employees of a public authority, the information in the records related to the performance of their positions and functions, as opposed to the positions and functions they held within the

¹⁶ [Decision 02/2019, Office of the Governor](#), paragraph 56.

Department. The exclusion in section 24(2)(a) thus did not apply to information about the CIO and the Department's staff in the relevant records.

93. Section 24(2)(b) also did not apply to information relating to a Cyberdine employee, because the service agreements that the Department had with Cyberdine as a company and not with the employee.¹⁷

[3] Whether any of the exceptions to the exemption in section 23(2) applied to the records?

94. None of the exceptions in section 23(2) applied to the relevant parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11. Specifically, the information concerned did not relate to the Applicant and the individuals to whom the information relates had not given written consent to disclosure of their personal information.

[4] If the exemption for personal information in section 23(1) was engaged, whether the balance of the public interest required disclosure?

95. There is a general public interest in the promotion of greater public understanding of the process or decisions of public authorities, accountability of and within the Government, as well as accountability for public expenditure. As the Applicant pointed out, based on the information available in the public domain, the value of the Government's service agreements with Cyberdine between August 2022 and June 2023 alone amounted to \$274,000. The records also related to an important subject, namely, the Government's management of its cybersecurity risks. Furthermore, the VCISO service provider plays a critical role in the management of such risks and the protection of the Government's IT system and various data (many of which relates to individuals and businesses) held in it. The public has a strong interest in knowing that critical service contracts are procured in accordance with existing procurement requirements. Because personal information is at issue, however, these public interest factors have to be weighed against the fairness and necessity of disclosure of such information.
96. In terms of fairness, the CIO as the Accounting Officer and the most senior public officer within the Department has, or should objectively have, expectations that some personal information relating to their work would be made available to the public, for transparency and accountability purposes. Disclosure of the CIO's name in records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 would therefore have been fair. Disclosure of the name and position of the CIO would also be necessary, as it would inform the public of the key individual in the

¹⁷ [Decision 12/2024](#), Ministry of Health Headquarters, paragraph 115.

management and protection of the data held by the Government of Bermuda in its IT system.

97. In contrast, disclosure of information about other officers or employees of the Department in the records would have been neither fair nor necessary. These individuals had reasonable expectations that their personal work information would not be disclosed to the public. Disclosure of their information would not have assisted the public with understanding the Department's decision making or promoted transparency around public spending. Similarly, disclosure of the signatures in records 1 and 2 would have been unfair, as doing so might put the relevant individuals at various risks such as forgery and identity theft.
98. Disclosure of the name and position of the Cyberdine employee who signed the Service Agreements in records 1 and 2 would have been fair because information about the individual's affiliation with Cyberdine was already available in the public domain. It would not have been fair, though, to disclose the name of a Cyberdine employee in records 3, 4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 because private company employees continue to have reasonable expectations of privacy. They are not accountable to the public in the same manner as the public officer who serves as the Accounting Officer. It is the Accounting Officer who is responsible to the public for the management of public sector contracts and the deliverables from a consultant. Disclosure of the name of the Cyberdine employee in records 3, 4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 would not further any public interest because they are an employee of a private company.

Conclusion

99. On her own accord the Information Commissioner has found that section 23(1) applied to parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11. The public interest required disclosure of the name and position of the CIO in the relevant records and the names and positions of individuals signing the Service Agreements in records 1 and 2.

Conclusions

100. The Information Commissioner finds that:
 - a. the Department did not conduct a reasonable search to locate records responsive to item 1c, but otherwise did so in accordance with section 12(2)(b) of the PATI Act and regulation 5 of the PATI Regulations,
 - b. the Department was not justified in relying on section 16(1)(f) to refuse public access to certain parts of records 1 and 2,

- c. the Department was not justified in relying on sections 30(1)(b) and 32(1)(a) to deny public access to records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11, once the actual deliverables were removed from the scope of the review and
- d. certain parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 were exempt under section 23(1). Save for the names and positions of the CIO and the names and positions of individuals signing the Service Agreements in records 1 and 2, disclosure of the personal information in the records was not in the public interest.

Decision

The Information Commissioner finds that the Information and Digital Technologies Department (**Department**) did not conduct a reasonable search in accordance with section 12 of the Public Access to Information (**PATI**) Act 2020 and regulation 5 of the PATI Regulations to locate records responsive to item 1c of the PATI request. The Information Commissioner further finds that the Department was not justified in relying on section 16(1)(f) to administratively deny access to certain parts of records 1 and 2 and on sections 30(1)(b) and 32(1)(a) to deny public access to the parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 still at issue in this review. Lastly, on her own accord, the Information Commissioner finds that parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 were exempt under section 23(1) but the public interest requires disclosure of certain personal information in the records.

In accordance with section 48 of the PATI Act, the Information Commissioner:

- annuls the Department’s decision on item 1c of the PATI request,
- varies the Department’s decision to deny public access to parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 by virtue of section 23(1), and
- reverses the Department’s decision to deny public access by relying on:
 - section 16(1)(f) for parts of records 1 and 2, and
 - sections 30(1)(b) and 32(1)(a) for the parts of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11 still at issue in this review, and
- orders the Department to disclose the remainder of records 1-4, 5.1, 6.1, 7.1, 8.1, 9.1, 10 and 11, with exempt information removed,

as directed by this Decision and the accompanying Confidential Annex and Order, which form part of this Decision, on or before **Friday, 6 September 2024**.

Judicial Review

The Applicant, the Information and Digital Technologies Department, the Third Party, or any person aggrieved by this Decision has the right to seek and apply for judicial review to the Supreme Court in accordance with section 49 of the PATI Act. Any such application must be made within six months of this Decision.

Enforcement

This Decision has been filed with the Supreme Court, in accordance with section 48(3) of the PATI Act. If the Department fails to comply with this Decision, the Information Commissioner has the authority to pursue enforcement in the same manner as an Order of the Supreme Court.

Gitanjali S. Gutierrez
Information Commissioner
26 July 2024

Appendix I: Relevant statutory provisions

Public Access to Information Act 2010

Access to records

- 12 (1) . . .
- (2) Public authorities shall make every reasonable effort to—
- ...
- (b) respond to requests completely, accurately and in a timely manner.
- ...

Refusal of request on administrative grounds

- 16 (1) A public authority may refuse to grant a request if—
- ...
- (f) the information is in the public domain, is reasonably accessible to the public, or is reasonably available to the public on request under any other statutory provision, whether free of charge or on payment; or
- ...

Public interest test

- 21 For the purposes of this Part, the test of whether disclosure by a public authority of a record or the existence of a record is in the public interest is whether the public interest would, on balance, be better served by disclosure than by non-disclosure.

Personal information

- 23 (1) Subject to the provisions of this section, a record that consists of personal information is exempt from disclosure.
- ...
- (6) A record that contains personal information relating to an individual shall be disclosed if disclosure of it is in the public interest or would benefit the individual.

Definition of personal information

- 24 (1) Subject to subsection (2), “personal information” means information recorded in any form about an identifiable individual, including—
- ...

Operations of public authorities

- 30 (1) Subject to subsection (2), a record is exempt if its disclosure could reasonably be expected to—
- ...
 - (b) have a significant, adverse effect on the performance by the public authority of any of its functions relating to management (including industrial relations and management of its staff); or
 - ...
- (2) A record shall be disclosed if disclosure of it is in the public interest.

National security, defence, and international relations

- 32 (1) Subject to subsection (3), a record is exempt from disclosure if—
- (a) disclosure of it would prejudice, or could reasonably be expected to prejudice, the security or defence of Bermuda or relations between Bermuda and any State or international organization of States; or
 - ...
- (3) A record shall be disclosed if disclosure of it is in the public interest.

Public Access to Information Regulations 2014

Reasonable search

- 5 (1) An information officer shall make reasonable efforts to locate a record that is the subject of an application for access.
- (2) Where an information officer has been unable to locate the record referred to in paragraph (1), he shall make a record of the efforts he made.

**Information Commissioner for Bermuda
Maxwell Roberts Building
4th Floor
One Church Street
Hamilton, HM 11
ico.bm
441-543-3700**