UK Anti-Doping
Fleetbank House
2-6 Salisbury Square
London EC4Y 8AE
T: +44 (0) 20 7842 3450
E: ukad@ukad.org.uk

[redacted]

Official

Ref : FOI-204

Sent via email only to:
[redacted]

18 September 2018

Dear [redacted]

1. Thank you for your email of 2 August 2018 in which you requested information from UK Anti-Doping ('UKAD') under the Freedom of Information Act 2000 ('the Act'). Your request was for information relating to cyber security incidents. Specifically, your request was as follows:

   I am writing to you under the Freedom of Information Act 2000 to request information regarding your organisation's diligence regarding cyber security.

   1. *Please may you inform me of how cyber or information security incidents were recorded by your organisation for the seven months from 1 January 2018 to 31 August 2018.*
   2. *Please provide me with the initial incident report and the official outcome report for these incidents.*

   The information sought regards breaches or contraventions of cyber or information security which necessarily reveals wrongdoing, and it is is [sic] in the public interest to understand their cause and effect.

   I trust you will find that the presumption towards disclosure favours the release of the information sought.

2. On 9 August 2018 we wrote to you and clarified the following:

   To clarify, UKAD is unable to respond with information for dates in the future. Therefore, UKAD will interpret the date range in your request as 1 January 2018 to 2 August 2018.

3. However, as 31 August has now passed, we confirm that UKAD has considered your request as per the period set out in your original email of 2 August, being the period 1 January 2018 to 31 August 2018.

4. On 10 August 2018 UKAD wrote to you seeking clarification. Our email was as follows:

   Namely, in the first part of your request are you asking for

   a. *How UKAD reported cyber or security incidents in the period between 1 January 2018 and 2 August 2018; or*

   b. *The amount of cyber or information security incidents reported between 1 January 2018 and 2 August 2018?*

   Can you please clarify if you are seeking the information in a) or b)?

5. You responded to the above request for clarification via email dated 13 August 2018. Your response was as follows:

   Thank you for writing seeking clarification. I am seeking both matter of information.

   Request A is a necessary component of request B. I would like to know the manner in which UKAD records and reports cyber security incidents, and I would like to know how many such incidents were reported.

Response

6. In regard to the manner in which UKAD records and reports cyber security incidents, we advise as follows:

   All security breaches or attempted security breaches, including information security breaches – be they cyber incidents or otherwise – are logged by the relevant "information risk owner" within the organisation. These incidents are logged on a central database which ensures that all relevant actions are taken to deal with the incident, including the following:

   a. that an incident report is given to any relevant parties;

   b. that an analysis of the incident occurs, including whether the incident has identified any vulnerabilities within UKAD's systems; and

   c. that, if any vulnerabilities are identified, these are promptly rectified.

7. UKAD confirms that there was one cyber incident in the period 1 January 2018 to 31 August 2018, which was an unsuccessful attack. We advise that, following a media report concerning this matter, UKAD issued a public statement which is available on our website here.

8. With respect to your request for the "incident report and the official outcome report", UKAD confirms that it holds one document that falls within the scope of your request, a redacted copy of which is enclosed. Pursuant to section 31 of the Act, UKAD has concluded that this document is partially exempt from disclosure, the rationale for which is set out below.

Section 31 – Law Enforcement

9. Section 31(1) of the Act states:

   Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—

   (a) the prevention or detection of crime…

10. UKAD has concluded that disclosure of the unredacted report would be likely to prejudice the prevention of crime, in that it would be likely to expose both UKAD and other organisations to cyber-attacks in future. This is because the redacted information, which includes matters such as the route of hacking and services effected, could be used by hackers to exploit vulnerabilities in UKAD's systems (or indeed other organisations) when planning and executing future attacks. Its disclosure is thus likely to prejudice the prevention of crime, being the prevention of future cyber-attacks.

11. Having concluded that disclosure of the unredacted report would be likely to prejudice the prevention of crime, UKAD has gone on to consider whether, despite this, the public interest nonetheless favours disclosure.

12. UKAD recognises the importance of transparency and accountability, including the advantages of public oversight of government processes and procedures and the management of cyber security issues. UKAD also acknowledges that there is a public interest in assuring the public that IT security issues are being taken seriously.

13. On the other hand, there is also a public interest in ensuring the continued effectiveness of UKAD's (and other organisations') cyber security systems and the protection of data (including third party personal data) held by those systems from

hackers. This is especially important given the sensitive personal data which UKAD holds, such as personal medical records.

14. Having considered the public interest arguments both for and against maintaining the exemption, UKAD has concluded that the balance of the public interest falls in favour of maintaining the exemption in this instance. In coming to this view, UKAD has taken account of the fact that the public interest arguments in favour of disclosure, as discussed above, are sufficiently met by the level of detail that is being disclosed. UKAD has also taken account of ICO decision notice fs50672471.

Conclusion

15. If you are dissatisfied with the handling of your request, you have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to: Philip Bunt, Chief Operating Officer, UK Anti-Doping, Fleetbank House, 2-6 Salisbury Square, London EC4Y 8AE. Please remember to quote the reference number above in any further communications.

16. If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely

UK Anti-Doping