[redacted]

From: FOI
Sent: 13 November 2023 08:42
To: [redacted]
Subject: FOI 120-23 - Response

Dear [redacted],

Our Ref: FOI 120-23

Thank you for your email to the Electoral Commission dated 10 August 2023.

The Commission aims to respond to requests for information promptly and regrets that is has not been able to do so within the statutory timeframe. The delay is a result of the high volume of Freedom of Information (FOI) requests received following the public announcement of the cyber-attack on 8 August 2023.

Your request is shown below followed by our response.

This is a FOI request relating to data breach, notified 8Aug 23.
Please advise further information on the data breach that is not present in the FAQ:
1/How many organisations, partners or separate gov.uk departments have permission to access EC data (of the sort that was compromised). Please list them all (including EC itself) with the following information:
a) Org name
b) Permitted Purpose(s) of org accessing data
c) Number of login ID's issued at the time of data breach
d) Login activity over the last one year
e) Whether any of org's login security was compromised or used in the data breach.
2/ whether method of entry to EC systems has been identified and whether a security weakness or failure has been identified. If so, please elaborate with details.
3/ whether, prior to this attack, EC had been advised on security practices by external organisations or government organisations (for example GCHQ) and whether advice received had been implemented in full. Please specify by advising organisation – including a table with columns of a)organisation b)date of (formal) advice c) date of EC compliance
4/ Whether T&C's relating to partner organisation access included terms relating to data security and whether there is any concern that such terms were not followed. List by org please.
5/ please provide the rationale (policy and process statements setting out the reasons) for aggregating data gathered at local level (eg by LA councils) into a central data base at EC level. Such data is normally expected to be used to issue voting forms and best practice might question why it need to be aggregated into a centralised dB – which it clearly is. Aggregate stats could easily be pulled in from local level without identifying individuals. Political donations could be cross checked by polling individual databases. There must have been discussions and concerns about generating a single database. Please provide details of those.
Now the suspicion must be that gov.uk is developing a national ID database ' on the side' without due process.
6/ what official response is being proposed to those who will (justifiably) say: "I am not going to return my yearly voter form (due this month ironically) because I cannot trust the government to keep my data safe. Instead, it will go in the bin".

7/ what is the reason for notifying the public on Aug 8th 2023 when the incident was identified in Oct 2022? Which organisations and persons were notified prior to August 8th 2023? Names and date of noitifications please (which should include individual HM Gov ministers if applicable).If the reason is the time to investigate, please provide list of organisations who have been involved in investigating and date of any reports they have provided.

Our Response:

Your request had several elements which we have addressed individually below with each element in *italics* followed by our response.

1/How many organisations, partners or separate gov.uk departments have permission to access EC data (of the sort that was compromised). Please list them all (including EC itself) with the following information:
a) Org name
b) Permitted Purpose(s) of org accessing data
c) Number of login ID's issued at the time of data breach
d) Login activity over the last one year
e) Whether any of org's login security was compromised or used in the data breach.

We hold this information, but section 21 of the FOI Act removes the need to provide it as it is reasonably accessible by other means.

FOI Act section 21

The Electoral Commission controls and processes data in order to carry out its statutory functions as explained in our privacy notices: Privacy policy | Electoral Commission.

The data that was compromised in the cyber-attack is described here: Public notification of cyber-attack on Electoral Commission systems | Electoral Commission.

It comprises personal data contained in:

- the electoral register and
- the email system of the Commission.

The Commission's processing of electoral registers is explained here: https://www.electoralcommission.org.uk/privacy-policy/electoral-registers. The Commission processes information from the registers to fulfil its functions but the controllers of particular registers are the Electoral Registration Officers (EROs) who are the primary controller of the Electoral Register in each Local Authority except Northern Ireland where the Electoral Office of Northern Ireland (EONI) performs that function. EROs and EONI publish their own privacy notices about the registers for which they are responsible.

The Commission's processing of personal data in the email system of the Commission in the context of the cyber-attack is explained here: https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems.

Providing you with links to information on our website in response to your request for information is permitted by section 21 of the FOI Act which removes the need to provide information in our response if it is reasonably accessible to an applicant by other means.

2/ whether method of entry to EC systems has been identified and whether a security weakness or failure has been identified. If so, please elaborate with details.

We hold this information but it is exempt from disclosure under section 31(1)(a) of the FOI Act. Section 31(1)(a) provides an exemption from disclosure that:

"would, or would be likely to, prejudice …the prevention or detection of crime".

The Commission's investigation into the cyber-attack includes sensitive, confidential information about the Commission's information technology systems and the nature of the attack on those systems. Disclosing sensitive, confidential information about our technology systems (such as methods of entry and identified security weaknesses or failures) would prejudice the security of our own systems and potentially also the security of similar systems used by other public bodies. Disclosure would be likely to prejudice the prevention and detection of similar cyber-attacks.

Section 31 is not an absolute exemption. The Commission must consider the factors in favour of disclosure and those against.

In this case, the public interest factors in disclosing the information are increased transparency about:

- the security of the Commission's IT systems and
- how the Commission has dealt with the data breach.

The public interest factors in withholding the information are protecting the integrity and security of the Electoral Commission's information technology systems and those of other public bodies with similar systems.

Having considered these factors, we are satisfied that on balance the public interest in maintaining the exemptions outweighs the public interest in disclosure at the present time.

3/ whether, prior to this attack, EC had been advised on security practices by external organisations or government organisations (for example GCHQ) and whether advice received had been implemented in full. Please specify by advising organisation – including a table with columns of a)organisation b)date of (formal) advice c) date of EC compliance

We hold this information but it is exempt under section 31(1)(g) of the FOI Act which provides an exemption where disclosure:

"would, or would be likely to, prejudice…the exercise by any public authority of its functions for any of the purposes specified in subsection (2)."

In this case the relevant purposes specified in subsection (2) are:

"(a) the purpose of ascertaining whether any person has failed to comply with the law…

(c) the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise…"

The Information Commissioner's Office's (ICO) investigation into the cyber-attack at the Electoral Commission is still ongoing. To release at this stage information about advice received in relation to the security of our systems and practices would, or would be likely to, prejudice the ICO's ability to conduct and conclude its investigation in a timely, fair and confidential manner.

Section 31 is not an absolute exemption. The Commission must consider the factors in favour of disclosure and those against.

In this case, the public interest factors in disclosing the information are increased transparency about:

- the security of the Commission's IT systems; and

- how the Commission dealt with the data breach.

The public interest factors in withholding the information are:

- protecting the integrity and security of the Electoral Commission's information technology systems and those of other public bodies;
- maintaining the ICO's ability to conduct investigations in a timely, fair and confidential manner;
- enabling organisations to engage openly with the ICO giving full disclosure of all relevant information without fear that information will be made public prematurely, or, as appropriate, at all.

Having considered these factors, we are satisfied that on balance the public interest in maintaining the exemption outweighs the public interest in disclosure at the present time (while the ICO's investigation is ongoing).

4/ Whether T&C's relating to partner organisation access included terms relating to data security and whether there is any concern that such terms were not followed. List by org please

We hold this information.

The Commission's arrangements for storing, processing and sharing data are under consideration by the ICO as part of their ongoing investigation into the cyber-attack.

Section 31(1)(g) of the FOI Act provides an exemption where disclosure:

*"would, or would be likely to, prejudice…the exercise by any public authority of its functions for any of the purposes specified in subsection (*2)."

In this case the relevant purposes specified in subsection (2) are:

"(a) the purpose of ascertaining whether any person has failed to comply with the law…

(c) the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise…"

Section 31 is not an absolute exemption. The Commission must consider the factors in favour of disclosure and those against.

In this case, the public interest factors in disclosing the information are increased transparency about the security of the Electoral Commission's IT systems.

The public interest factors in withholding the information are maintaining the ICO's ability to conduct investigations in a timely, fair and confidential manner; and enabling organisations to engage openly with the ICO giving full disclosure of all relevant information without fear that information will be made public prematurely, or, as appropriate, at all.

Having considered these factors, we are satisfied that on balance the public interest in maintaining the exemption outweighs the public interest in disclosure at the present time (while the ICO's investigation is ongoing).

5/ please provide the rationale (policy and process statements setting out the reasons) for aggregating data gathered at local level (eg by LA councils) into a central data base at EC level. Such data is normally expected

to be used to issue voting forms and best practice might question why it need to be aggregated into a centralised dB – which it clearly is. Aggregate stats could easily be pulled in from local level without identifying individuals. Political donations could be cross checked by polling individual databases. There must have been discussions and concerns about generating a single database. Please provide details of those.
Now the suspicion must be that gov.uk is developing a national ID database ' on the side' without due process.

As is stated within the Privacy Notices, Electoral Registration Officers have a legal obligation to share the full electoral registers collected for Local Government Elections, UK Parliamentary Elections, and elections to the Scottish and Welsh Parliaments with a number of organisations including the Electoral Commission. The Commission collects and stores the Register of Electors in pursuance to its legal functions under the Political Parties Elections Referendums Act 2000 (PPERA), including by checking whether donations accepted, and transactions entered into by, registered political parties are permissible under the law and considering enforcement action under PPERA if they are not.

There are two legal bases for processing electoral register data. The Commission process the information as part of its public task or in the exercise of our official authority under our statutory functions in PPERA.

6/ what official response is being proposed to those who will (justifiably) say: "I am not going to return my yearly voter form (due this month ironically) because I cannot trust the government to keep my data safe. Instead, it will go in the bin".

The canvass forms are not issued by the Electoral Commission. They are administered and issued by the Local Authority and Electoral Registration Officers. We would suggest you contact your local Electoral Registration Office for this information.

7/ what is the reason for notifying the public on Aug 8th 2023 when the incident was identified in Oct 2022? Which organisations and persons were notified prior to August 8th 2023? Names and date of notifications please (which should include individual HM Gov ministers if applicable). If the reason is the time to investigate, please provide list of organisations who have been involved in investigating and date of any reports they have provided.

We hold this information.

Information about the steps we took and the timing of the announcement is available here: https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems/information-about-cyber-attack.

The Commission's response to the cyber-attack is currently under consideration by the ICO for the purpose of their independent investigation and preparation of their report.

Information about the root cause of the attack is exempt from disclosure under section 31(1)(g) at the present time and the public interest in maintaining the exemption outweighs the public interest in disclosure.

Section 31(1)(g) provides an exemption where disclosure:

"would, or would be likely to, prejudice…the exercise by any public authority of its functions for any of the purposes specified in subsection (2)."

In this case the relevant purposes specified in subsection (2) are:

"(a) the purpose of ascertaining whether any person has failed to comply with the law…

(c) the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise…"

The ICO's investigation into the cyber-attack at the Electoral Commission is still ongoing. To release at this stage information about the root cause of the attack would, or would be likely to, prejudice the ICO's ability to conduct and conclude its investigation in a timely, fair and confidential manner.

Section 31 is not an absolute exemption. The Commission must consider the factors in favour of disclosure and those against.

In this case, the public interest factors in disclosing the information are increased transparency about the security of the Commission's IT systems.

The public interest factors in withholding the information are maintaining the ICO's ability to conduct investigations in a timely, fair and confidential manner; and enabling organisations to engage openly with the ICO giving full disclosure of all relevant information without fear that information will be made public prematurely, or, as appropriate, at all.

Having considered these factors, we are satisfied that on balance the public interest in maintaining the exemption outweighs the public interest in disclosure at the present time (while the ICO's investigation is ongoing).

I trust that this information satisfies your request. The Commission strives to be an open, transparent authority, but in some circumstances we cannot responsibly release requested information, and we ask for your understanding in this regard.

If you are not satisfied with this response, please note that the Commission operates a review procedure, details of which can be found on the Commission website at: https://www.electoralcommission.org.uk/freedom-information/make-a-freedom-information-request.

Please also note that if you have exhausted all internal Commission review procedures and you are still not satisfied you have the right to appeal to the Information Commissioner. Details of this procedure can be found on the ICO website: https://ico.org.uk/.

Yours sincerely

Information Officer
FOI@electoralcommission.org.uk

The Electoral Commission
electoralcommission.org.uk