Freedom of Information Team
Correspondence Unit
9 Downing Street
SW1A 2AG

foi@dexeu.gov.uk
www.gov.uk

Don Priest
Via: request-562429-2160d242@whatdotheyknow.com

Our ref: FOI2019/02778
15 April 2019

Dear Mr Priest,

We refer to your request of 18 March 2019, where you asked:

'Qu 1 What security rules, codes, protocols, procedures and precautions are taken to ensure that the CIA, GCHQ /Cabinet office are not eavesdropping / spying on staff, officials and ministers in your Department with social media eg Google, Facebook as a conduit?

Qu 2 What summaries / reports does the department have about its cyber security? Please indicate the public facing reports.
.
Qu 3 Has the Department risk assessed the threat posed by social media, especially that owned by foreign corporations and countries and especially US and CIA? What summaries does the department have of this information, including any public facing ones?

Qu 4 What social media apps are allowed on the Departments phones and computers? Which are installed?

Qu 5 Are Facebook, Google and Twitter apps allowed to be installed and or used on Department computers and mobile phones?

Qu 6 Are private, ie individually owned, mobile phones and computers with social media apps installed such as Facebook, Google and Twitter allowed in Department meetings, committees, and in the office environment?

Qu 8 If the answer to Qu 5 and Qu 6 are yes, how does the Department stop companies / CIA spying utilising microphones, cameras, and GPS data on those devices?

Qu 9 Has the department informed staff of the risk of spying and eavesdropping via social media apps? If so please send a copy of the memo / paper.

Qu 10 Has the Department contributed material to the Cabinet Office as part of the cyber security strategy? If so what?

Questions on Q sometimes written as QAnon, #Q #QAnon

(Background information on Q follows the questions)

Qu 11 Has the Secretary, Ministers or the top 3 civil servants in the Department been briefed about QAnon?

Qu 12 If so please indicate the date and the type of recorded information that has been briefed so that any future request may be narrowed down, as per Section 16 of the UK freedom of Information Act and Information Commissioner Guidance.

Qu 13 Has the Department any other recorded information on Q / QAnon ? If so please indicate the date and the type of recorded information that has been briefed so that any future request may be narrowed down, as per Section 16 of the UK freedom of Information Act and Information Commissioner Guidance. (If there is a mass of information that will take the request over the time limit, please disregard this question)'

Your request has been treated under the Freedom of Information Act 2000 ('the Act'). Our response to each question is provided below:

1. It is not entirely clear what recorded information you are requesting, however, we can confirm that the Department for Exiting the European Union (DExEU) has various internal security policies and procedures in place to guard against cyber security and general security threats. Members of staff are also provided with a security briefing when they join the department, which covers the personal use of social media.

2. The Department for Exiting the European Union (DExEU) does not hold any information relevant to this request.

3. In accordance with section 24(2) (National Security) and section 31(3) (Law Enforcement) of the Act, I can neither confirm nor deny whether DExEU holds any information in scope of this part of your request. Under section 24(2) of the Act, the duty to confirm or deny does not arise if, or to the extent that, exemption from the duty to confirm or deny is required for the purpose of safeguarding national security. Under section 31(3) of the Act, the duty to confirm or deny does not arise if, or to the extent that, compliance with the duty to confirm or deny would, or would be likely to, prejudice any of the matters mentioned in section 31(1) of the Act. Confirming or denying whether we hold information of the type you requested would be likely to prejudice (a) the prevention or detection of crime and (b) the apprehension or prosecution of offenders. We have considered the public interest factors in favour of, and against, disclosing the requested information below.

4. The following social media apps are available on the work phones of DExEU staff members: Twitter, Instagram and YouTube.

5. Please see the response given above to 'question 4'.

6. There are security policies in place which stipulate when and where personal phones are and are not allowed in the workplace.

8. Please refer to the response given above for ‘question 1’.

9. DExEU provides new staff members with security inductions, including on the personal use of social media when they join the department.

10. DExEU has not contributed material to the Cabinet Office as part of the Cyber Security Strategy. The strategy was published in November 2016 and DExEU was created only shortly before that in July 2016.

11. 12. and 13. Please see our response to question 3. Further explanation of the application of these exemptions and the relevant public interest tests are provided below.

Section 24(2)

Section 24(2) of the Act confirms that the duty to confirm or deny the existence of information is exempt where required for the purpose of safeguarding national security.

Section 24 is a qualified exemption and we have considered whether the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in confirming whether or not DExEU holds any information relating to your request.

Public Interest Test:

DExEU recognises that openness in government may increase public trust in and engagement with government, especially when it relates to security matters. We also recognise the public have a natural concern that the measures in place to safeguard national security are effective.

Opposing this, there is a very strong public interest in safeguarding national security. It would be contrary to this public interest to confirm or deny whether any information is held where to do so would undermine the effective safeguarding of national security or related measures. In particular, confirming or denying what particular areas of security have or have not been risk assessed or analysed for briefing senior staff and Ministers would allow individuals to build a picture of where strengths and weaknesses in departmental security might exist by publicly identifying areas of interest or non-interest. This would help those wishing to undermine DExEU security.

Taking into account all the circumstances of this case, we have concluded that the public interest favours maintaining the exclusion of the duty to confirm or deny whether we hold information in relation to your request.

Section 31(3)

Section 31(3) of the Act confirms that the duty to confirm or deny does not arise if to do so would, or would be likely to, prejudice any of the matters mentioned in section 31(1)(a) and (b), namely the prevention or detection of crime and the apprehension or prosecution of offenders.

Section 31 is a qualified exemption and we have considered whether the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in confirming whether or not DExEU holds any information relating to your request.

Public Interest Test

DExEU recognises that there is a general public interest in disclosure of information and recognises that openness in government may increase public trust in and engagement with government. We also recognise a public interest in assuring the public that effective arrangements are in place for departmental security, particularly where matters might be linked to law enforcement.

Opposing this, there is a very strong public interest in the prevention and detection of crime. It is contrary to the public interest to disclose information which would assist the facilitation of crime or hinder its detection. Information security is in place to safeguard DExEU information assets, and in confirming or denying if we held the information you have requested, we may undermine such departmental security. Particularly, as stated under section 24 arguments , confirming or denying what particular areas of security have or have not been risk assessed or analysed for briefing senior staff and Ministers would allow individuals to build a picture of where strengths and weaknesses in departmental security might exist by publicly identifying areas of interest or non-interest. This would help those wishing to undermine DExEU security.

Taking into account all the circumstances of this case, we have concluded that the public interest favours maintaining the exclusion of the duty to confirm or deny whether we hold information in relation to your request.

If you have any queries about this letter, please contact the FOI team. Please remember to quote the reference number above in any future communications.

If you are unhappy with the service you have received in relation to your request or wish to request an internal review, you should write to foiappeals@dexeu.gov.uk or:

Freedom of Information Team (internal review)
Department for Exiting the European Union
9 Downing Street
SW1A 2AG

You should note that DExEU will not normally accept an application for internal review if it is received more than two months after the date that the reply was issued.

If you are not content with the outcome of your internal review, you may apply directly to the Information Commissioner for a decision. Generally, the Commissioner cannot make a decision unless you have exhausted the complaints procedure provided by DExEU. The Information Commissioner can be contacted at:

The Information Commissioner's Office

Wilmslow
Cheshire
SK9 5AF

Yours faithfully

Freedom of Information Team, DExEU.