Ministry
of Defence Police

MDP Secretariat
Room 126, Building 1070
MDP HQ Wethersfield
Braintree, Essex CM7 4AZ

Tel: 01371 85[redacted]

E-mail: MDP-FOI-DP@mod.gov.uk

[redacted]

[redacted]

Our Ref: eCase: FOI2018/06625 RFI:149/18
Date: 03 July 2018

Dear [redacted]

FREEDOM OF INFORMATION ACT 2000: MINISTRY OF DEFENCE POLICE: GDPR COMPLIANCE

We refer to your email dated 16 May 2018 which was acknowledged on same date.

We are treating your email as a request for information in accordance with the Freedom of Information Act 2000 (FOIA 2000).

In your email, you requested the following information:

"1. Have you invested in technology specifically to comply with GDPR?
o Yes
o No

2. Which information security framework(s) have you implemented?

3. Have you signed contractual assurances from all the third-party organisations you work with requiring that they achieve GDPR compliance by 25 May 2018?
o Yes
o No

4. Have you completed an audit to identify all files or databases that include personally identifiable information (PII) within your organisation?
o Yes
o No

5. Do you use encryption to protect all PII repositories within your organisation?
o Yes
o No

6. As part of this audit, did you clarify if PII data is being stored on, and/or accessed by:
a. Mobile devices
b. Cloud services
c. Third party contractors

7. Does the organisation employ controls that will prevent an unknown device accessing PII repositories?
o Yes
o No

8. Does your organisation employ controls that detect the security posture of a device before granting access to network resources – i.e. valid certificates, patched, AV protected, etc.
o Yes
o No

9. Should PII data be compromised, have you defined a process so you can notify the relevant supervisory authority within 72 hours?
o Yes
o No

10. Have you ever paid a ransom demand to have data returned / malware (aka ransomware) removed from systems?
o Yes
o No

11. To which positions/level does your data protection officer report? i.e. CISO, CEO, etc.

12. How many company computing devices (aka smartphones, tablets, laptops, computers) were reported lost and/or stolen in 2017?

13. How many people have been prosecuted under the 'Misuse of Computers Act' in your region in the last 12 months? Of these how many resulted in a conviction?"

A search for information has now been completed by the Ministry of Defence Police (MDP) and I can confirm that we do hold some information in scope of your request.

1. Have you invested in technology specifically to comply with GDPR?

Yes

2. Which information security framework(s) have you implemented?

In relation to question 2 I am exempting any information relevant to your request as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemption:

Section 31(3) – Law enforcement

Section 31(3) is prejudice based qualified exemption and there is a requirement to

articulate the harm that would be caused in releasing the information by carrying out a Public Interest Test .

Section 31 (1) applies because if we were to release the information requested in relation to this question it could provide those persons with criminal intent with intelligence which may assist them with the ability to hack into our policing systems, or on a wider scale, the MOD systems, and compromise investigations and potentially the security of the country.

3. Have you signed contractual assurances from all the third-party organisations you work with requiring that they achieve GDPR compliance by 25 May 2018?

No

4. Have you completed an audit to identify all files or databases that include personally identifiable information (PII) within your organisation?

Yes

5. Do you use encryption to protect all PII repositories within your organisation?

No

6. As part of this audit, did you clarify if PII data is being stored on, and/or accessed by:
a. Mobile devices
b. Cloud services
c. Third party contractors

Yes

7. Does the organisation employ controls that will prevent an unknown device accessing PII repositories?

Yes

8. Does your organisation employ controls that detect the security posture of a device before granting access to network resources – i.e. valid certificates, patched, AV protected, etc.

In relation to question 8 I am exempting any information relevant to your request as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemption:

Section 31(3) – Law enforcement

Section 31(3) is prejudice based qualified exemption and there is a requirement to articulate the harm that would be caused in releasing the information by carrying out a Public Interest Test.

Section 31 (1) applies because if we were to release the information requested in relation to this question it could provide those persons with criminal intent with intelligence

which may assist them with the ability to hack into our policing systems, or on a wider scale, the MOD systems, and compromise investigations and potentially the security of the country.

9. Should PII data be compromised, have you defined a process so you can notify the relevant supervisory authority within 72 hours?

Yes

10. Have you ever paid a ransom demand to have data returned / malware (aka ransomware) removed from systems?

In relation to question 10 the MDP can neither confirm nor deny that it holds any information relevant to your request as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemption:

Section 31(3) – Law enforcement

Section 31(3) is prejudice based qualified exemption and there is a requirement to articulate the harm that would be caused in confirming or not that the information is held as well as carrying out a public interest test.

I have conducted a public interest test and concluded that the balance strongly favours neither confirming or denying the Ministry of Defence Police holds information.

Section 31(3) applies because confirming or denying if information is held would be likely to impact upon law enforcement. To confirm or deny specific details of any breaches of information technology and security would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

This should not be taken as conclusive evidence that any information that would meet your request exists or does not exist.

11. To which positions/level does your data protection officer report? i.e. CISO, CEO, etc.

The Senior Information Risk owner

12. How many company computing devices (aka smartphones, tablets, laptops, computers) were reported lost and/or stolen in 2017?

None

13. How many people have been prosecuted under the 'Misuse of Computers Act' in your region in the last 12 months? Of these how many resulted in a conviction?

The Ministry of Defence Police have had no prosecutions under the 'Misuse of Computers Act' in the last 12 months.

If you have any queries regarding the content of this letter, please contact this office in the first instance.

If you are not satisfied with this response or wish to complain about any aspect of the handling of your request, then you should contact me in the first instance. If informal resolution is not possible and you are still dissatisfied then you may apply for an independent internal review by contacting the Information Rights Compliance team, Ground Floor Zone D, MOD Main Building, Whitehall, London SW1A 2HB (email CIO-FOI-IR@mod.gov.uk). Please note that any request for an internal review must be made within 40 working days of the date on which the attempt to reach informal resolution has come to an end.

If you remain dissatisfied following an internal review, you may take your complaint to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not investigate the case until the MOD internal review process has been completed. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website (http://www.ico.org.uk).

Yours sincerely

MDP Sec Data Protection and Freedom of Information Office