Freedom of Information Request Reference N^{o}: FOI 001731-18

I write in connection with your request for information received by Norfolk and Suffolk Constabularies on the 16 May 2018 in which you sought access to the following information:

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

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

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

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

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

- *Yes*
- *No*

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

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

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

Response to your Request

The response provided below is correct as of 21 May 2018

Norfolk and Suffolk Constabularies have considered your request for information and our response is below.

1. Suffolk and Norfolk Constabularies have not invested in technology specifically to comply with GDPR.

2. Information concerning the Constabularies security framework has not been provided due to exemptions within the Act.

   Section 17 of the Freedom of Information Act 2000 requires that Suffolk and Norfolk Constabularies, when refusing to provide such information (because the information is exempt) is to provide you, the applicant, with a notice ban which:

   (a) States that fact
   (b) Specifies the exemption(s) in question and
   (c) States (if that would not otherwise be apparent) why the exemption(s) applies.

   The information is exempt from disclosure by virtue of the following exemption;

   - **Section 31(1) – Law Enforcement**

   Section 31 is a qualified and prejudice based exemption and I am therefore obliged to consider the harm in providing the information and conduct a public interest test.

3. Suffolk and Norfolk Constabularies are in the final stages of this work.

4. We have completed an audit to identify all files or databases that include personally identifiable information.

5. We do use encryption to protect all PII repositories.

6. We did clarify if PII data is being stored on, and/or accessed by these devices, services and contractors.

7. The Constabularies do not permit unknown devices to connect to our network.

8. Information concerning the controls employed to detect the security posture of a device before granting access to network resources has not been provided as a result of exemptions within the Act.

   Section 17 of the Freedom of Information Act 2000 requires that Suffolk and Norfolk Constabularies, when refusing to provide such information (because the information is exempt) is to provide you, the applicant, with a notice ban which:

   (a) States that fact
   (b) Specifies the exemption(s) in question and
   (c) States (if that would not otherwise be apparent) why the exemption(s) applies.

   The information is exempt from disclosure by virtue of the following exemption;

   - **Section 31(1) – Law Enforcement**

   Section 31 is a qualified and prejudice based exemption and I am therefore obliged to consider the harm in providing the information and conduct a public interest test.

9. The Constabularies have defined such a process.

10. Suffolk and Norfolk Constabularies can neither confirm nor deny whether any ransom demands have or have not been received and whether or not such a ransom has been paid.

    The Constabularies can neither confirm nor deny that it holds the information you have requested as the duty in s1(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 is a qualified and prejudice based exemption and I am therefore obliged to consider the harm in confirming or denying whether any information is held and conduct a public interest test.

11. The Data Protection Officer reports to a Chief Officer.

Section 31(1) – Harm and Public Interest Test

Harm

Information relating to the Constabularies Security Framework and controls that detect the security of devices will enable individuals to research the Constabularies and compromise the Constabularies IT systems and force Infrastructure. This could lead to attacks on the Constabularies systems including data theft, denial of service attacks and other deliberate disruptions.

Disclosure of such information would lead to a significantly increased risk of a security compromise by a malicious act against our infrastructure. Should the security compromise actually be successful, the harm caused would include a compromise of the forces ability to use its own ICT, potentially leading to direct harm to members of the public.

The Constabularies have a duty to enforce the law and protect the public. Disclosure under the Freedom of Information Act (FOIA) could be used to identify where there are potential weaknesses in security products and target specific areas, this could lead to a security risk to systems. This would consequently undermine the Police Service's law enforcement capability.

Factors favouring disclosure

Provision of the information would allow a greater understanding of where public funds are being allocated. For the Police Service to be fully transparent and open, it is appreciated that there is a public interest in providing information that infers where public money may be spent.

Factors against disclosure

Provision of such information would allow individuals to utilise the data in a discovery phase of a potential attack, which would leave the Constabularies network vulnerable.

The IT infrastructure is vital to the ability of the Constabularies to effectively prevent and detect crime, share data and maintain a proficient law enforcement capacity. Information will not be disclosed if it such would compromise that capability in any way and expose the Constabularies to attack. Any disruption to Constabulary systems would result in the need for additional resources and increased expenditure to ensure that policing activities are not compromised or data lost. There would also be a requirement for additional funds to carry out repairs and system recovery.

Policing resources and the police capability would be negatively affected, and manipulated by those with criminal intent, to obtain an advantage over any potential police tactics and capabilities. In a world where cybercrime is ever increasing it is of paramount importance to protect such sensitive information.

Balance Test

The points above highlight the merits of confirming information held however, the Police Service will never divulge information if to do so would undermine law enforcement capabilities. Whilst there is a public interest in the transparency in how the Police Service delivers effective law enforcement and ensures information security, there is a strong public interest in safeguarding police systems and information.

Whilst there is a public interest in the transparency and accountability, there is a very strong public interest in safeguarding information that may imply vulnerabilities or weaknesses that individuals may use to try and focus efforts on to attack the Constabulary IT Infrastructure

The security of force systems is of paramount importance and this should not be jeopardised by the any release of information under the Freedom of Information Act. Therefore, at this moment in time, it is our opinion that the balance test for the information requested is not provided and the exemption at Section 31 is engaged.

Section 31(3) – Harm and Public Interest Test

Harm

Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply with statutory requirements, the College of Policing Authorised Professional Practice (APP) for Information Assurance, has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see link below:-

https://www.app.college.police.uk/app-content/information-management/

To confirm or deny whether any ransom has or has not been paid would invariably identify whether the Constabularies have vulnerable computer systems and provide actual knowledge of whether attacks have or have not taken place within individual force areas.

It is vitally important that information sharing takes place with other police forces and security bodies within the UK to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime.

To confirm or deny specific details of any ransomware attacks would be extremely useful to those involved in terrorist activity as it would enable those involved in such activity to map vulnerable information security databases.

Public Interest Test

Factors favouring confirmation or denial of whether information is held

Confirming that information exists, relevant to this request, would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce attacks.

Factors against confirmation or denial of whether information is held

Confirmation or denial of whether information exists in this case would suggest that Norfolk and Suffolk Constabularies take their responsibility to protect information and information systems from unauthorised access, destruction, etc, dismissively and inappropriately.

Balance Test

The points above highlight the merits of confirming or denying whether the requested information exists. The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive, relating to high profile investigative activity.

In order to comply with statutory requirements and to meet the NPCC expectation of the Police Service, with regard to the management of information security, a national policy approved by the College of Policing, titled National Policing Community Security Policy, has been put in place. This policy has been constructed to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations. A copy of this can be accessed via the below link:-

http://library.college.police.uk/docs/APP-Community-Security-Policy-2014.pdf

In addition, anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service. Therefore, at this moment in time, it is our opinion that for these reasons the balance test favours neither confirming nor denying whether information is held.

No inference should be taken from this response as to whether information does or does not exist.

Should you have any further queries concerning this request, please contact Clair Pack, FOI Decision Maker, quoting the reference number shown above.

A full copy of the Freedom of Information Act (2000) can be viewed on the 'Office of Public Sector Information' web-site;
http://www.opsi.gov.uk/

Norfolk and Suffolk Constabularies are not responsible for the content, or the reliability, of the website referenced. The Constabulary cannot guarantee that this link will work all of the time, and we have no control over the availability of the linked pages.

Your Right to Request a Review of Decisions Made Under the Terms of the Freedom of Information Act (2000).

If you are unhappy with how your request has been handled, or if you think the decision is incorrect, you have the right to ask the Norfolk and Suffolk Constabulary to review their decision.

Ask Norfolk and Suffolk Constabularies to look at the decision again.

If you are dissatisfied with the decision made by Norfolk and Suffolk Constabularies under the Freedom of Information Act (2000), regarding access to information, you must notify the Norfolk and Suffolk Constabulary that you are requesting a review within 20 days of the date of its response to your Freedom of Information request. Requests for a review should be made in writing and addressed to:

Freedom of Information Decision Maker
Information Management Department
Suffolk Constabulary
Police Headquarters
Martlesham Heath
Ipswich
Suffolk
IP5 3QS
OR
Email: information@suffolk.pnn.police.uk

In all possible circumstances Norfolk and Suffolk Constabulary will aim to respond to your request for us to look at our decision again within 20 working days of receipt of your request for an internal review.

The Information Commissioner.

After lodging a request for a review with Norfolk and Suffolk Constabulary, if you are still dissatisfied with the decision, you can apply to the Information Commissioner for a decision on whether the request for information has been dealt with in accordance with the requirements of the Act.

For information on how to make application to the Information Commissioner please visit their website at www.ico.org.uk or contact them at the address shown below:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 01625 545 700