Human Tissue Authority
2nd Floor
2 Redman Place
London
E20 1JQ

Tel 020 7269 1900
Web www.hta.gov.uk
Email enquiries@hta.gov.uk

Date: 22 October 2021

By email to: [redacted]

Dear [redacted]

Freedom of Information request

Thank you for your request for information under the Freedom of Information Act (FOIA), which was received by the Human Tissue Authority (HTA) on Thursday 23 September 2021. Your email outlined the following request:

I am writing to you under the Freedom of Information Act 2000 to request the following information from Human Tissue Authority. Please can you answer the following questions:

1. In the past three years has your organisation:

   a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)
      i. If yes, how many?

   b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)

   c. Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)

   d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?
      i. If yes was the decryption successful, with all files recovered?

   e. Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)?
      i. If yes was the decryption successful, with all files recovered?

f. Had a formal policy on ransomware payment?
    i. If yes please provide, or link, to all versions relevant to the 3 year period.

g. Held meetings where policy on paying ransomware was discussed?

h. Paid consultancy fees for malware, ransomware, or system intrusion investigation
    i. If yes at what cost in each year?

i. Used existing support contracts for malware, ransomware, or system intrusion investigation?

j. Requested central government support for malware, ransomware, or system intrusion investigation?

k. Paid for data recovery services?
    i. If yes at what cost in each year?

l. Used existing contracts for data recovery services?

m. Replaced IT infrastructure such as servers that have been compromised by malware?
    i. If yes at what cost in each year?

n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?
i. If yes at what cost in each year?

o. Lost data due to portable electronic devices being mislaid, lost or destroyed?
    i. If yes how many incidents in each year?

2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?

    a. If yes is this system's data independently backed up, separately from that platform's own tools?

    b. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)

    a. Mobile devices such as phones and tablet computers
    b. Desktop and laptop computers
    c. Virtual desktops
    d. Servers on premise
    e. Co-located or hosted servers
    f. Cloud hosted servers
    g. Virtual machines
    h. Data in SaaS applications

i. ERP / finance system
j. We do not use any offsite back-up systems

4. Are the services in question 3 backed up by a single system or are multiple systems used?

5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?

6. How many Software as a Services (SaaS) applications are in place within your organisation?
    a. How many have been adopted since January 2020?

Please provide the information requested in the form of an email.

If it is not possible to provide the information requested due to the information exceeding the cost of compliance limits identified in Section 12, please provide advice and assistance, under the Section 16 obligations of the Act, as to how I can refine my request.

If you can identify any ways that my request could be refined I would be grateful for any further advice and assistance.

If you have any queries please don't hesitate to contact me via email or phone and I will be happy to clarify what I am asking for and discuss the request, my details are below.

Clarifications

I wrote to you via email on Friday 3 September 2021 to request the following clarification:

To assist with this request, can you please clarify if the information you are seeking is for the calendar year from 2018-2020 inclusive or the financial year starting from 2018?

You responded via email on Thursday 23 September 2021 to confirm:

As analysing records to fit a time window not used internally would be time consuming we would be happy with receiving information on the period you normal record that offer the best overlap with the calendar years.

As the HTA internal reports are based on the financial year, this is what we have based our response to you on.

Response

1. In the past three years has your organisation:

   a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?) i. If yes, how many?

      We have not experienced any ransomware incidents.

   b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)

      We have not had any data rendered permanently inaccessible by a ransomware incident.

   c. Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)

      We have not had data rendered permanently inaccessible by a systems or equipment failure.

   d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool? i. If yes was the decryption successful, with all files recovered?

      We have not paid any ransom due to a ransomware incident or to obtain a decryption key or tool.

   e. Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)? i. If yes was the decryption successful, with all files recovered?

      We have not used a free decryption key or tool.

   f. Had a formal policy on ransomware payment? i. If yes please provide, or link, to all versions relevant to the 3 year period.

      We do not have a formal policy on ransomware payment.

   g. Held meetings where policy on paying ransomware was discussed?

      We have not held meetings where policy on paying ransomware was discussed.

   h. Paid consultancy fees for malware, ransomware, or system intrusion investigation i. If yes at what cost in each year?

We have not paid consultancy fees for malware, ransomware, or system intrusion investigation.

i. Used existing support contracts for malware, ransomware, or system intrusion investigation?

   We have used our existing managed support contract to supplement our own malware, ransomware, or system intrusion investigation.

j. Requested central government support for malware, ransomware, or system intrusion investigation?

   We have not requested central government support for malware, ransomware, or system intrusion investigation.

k. Paid for data recovery services? i. If yes at what cost in each year?

   We have not paid for data recovery services.

l. Used existing contracts for data recovery services?

   We have not used existing contracts for data recovery services.

m. Replaced IT infrastructure such as servers that have been compromised by malware? i. If yes at what cost in each year?

   We have not needed to replace any IT infrastructure compromised by malware because none have been compromised by malware.

n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware? i. If yes at what cost in each year?

   We have not needed to replace any IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware because none have been compromised by malware.

o. Lost data due to portable electronic devices being mislaid, lost or destroyed? i. If yes how many incidents in each year?

   We have not lost data due to portable electronic devices being mislaid, lost or destroyed.

2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?

   We use Microsoft Office 365.

   a. If yes is this system's data independently backed up, separately from that platform's own tools?

Yes, this system's data independently backed up, separately from that platform's own tools.

3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)

   a. Mobile devices such as phones and tablet computers

      Any data accessed on these devices originates from the HTA Microsoft 365 tenant which is backed up offsite.

   b. Desktop and laptop computers

      Any data accessed on these devices originates from the HTA Microsoft 365 tenant which is backed up offsite.

   c. Virtual desktops

      We do not use virtual desktops.

   d. Servers on premise

      We do not have any servers on premise.

   e. Co-located or hosted servers

      Our hosted servers are the target for our offsite backups.

   f. Cloud hosted servers

      Data on our cloud hosted virtual servers are backed up offsite.

   g. Virtual machines

      See above.

   h. Data in SaaS applications

      Data in SaaS applications is subject to the backup strategy of the SaaS application vendor.

   i. ERP / finance system

      Our finance system data is backed up offsite.

   j. We do not use any offsite back-up systems

4. Are the services in question 3 backed up by a single system or are multiple systems used?

A single system is used to backup the data.

5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?

   Our cloud migration strategy has completed and we are now fully in the cloud.

6. How many Software as a Services (SaaS) applications are in place within your organisation?

   There are five SaaS applications in place at the HTA.

   a. How many have been adopted since January 2020?

   Two SaaS applications have been adopted since January 2020.

Further information

If you are unhappy with the way the HTA has handled your request for information in this case, you may in the first instance ask us for an internal review by writing to us at the above postal or email address.

If you remain dissatisfied with the handling of your request, you have the right to appeal directly to the Information Commissioner for a decision, at the address below. There is no charge for making an appeal.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Telephone: 08456 30 60 60 or 01625 54 57 45
Website: www.ico.gov.uk

Yours sincerely

[redacted]