Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Southampton City Council
Civic Centre
Southampton
SO14 7LY

By email only to: [redacted]

Date: 30 June 2022

Dear [redacted]

Case Reference Number: INV/0516/2020

I write further to your latest correspondence to the ICO of 8 October 2021. In this, you provided a response to the ICO's further enquiries of 27 September 2021.

I write to inform you that the ICO has now reached a decision in respect of its investigation into INV/0516/2020.

This investigation concerns Southampton City Council's (SCC) policy requirement that all licensed taxis, and the majority of private hire vehicles (PHVs), be fitted with a CCTV system that is in permanent operation. This policy results in the continuous recording of all drivers and their passengers in taxis and PHVs licensed by SCC whenever they are in use, to include when that use is for private purposes.

This case has been considered under the United Kingdom General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018 (the DPA 2018) due to the nature of the processing involved. We refer to the UK GDPR and the DPA 2018 together as the 'data protection legislation'.

Our consideration of this case

As you are aware, the ICO previously submitted a Preliminary Enforcement Notice (PEN) to SCC on 4 September 2019. This outlined the Commissioner's intention to issue SCC with an Enforcement Notice (EN) for infringements of Article 5(1)(a) and Article 5(1)(c) of the GDPR.

A further breach of Schedule 1, Part I, Article 8 of the Human Rights Act 1998 was also identified; which in turn amounted to a breach of the fairness requirement of Article 5(1)(a). This is because the latter requires a balancing exercise which takes into account the justification for the data processing and the potential harmful impact on individuals.

Since issuing its PEN to SCC, representations from SCC in respect of this notice were received on 4 October 2019. A site visit was also undertaken by the ICO's Civil Investigations team, and a series of further enquiries were posed to SCC.

The ICO also wishes to highlight its publication of updated video surveillance guidance in early 2022.

Investigation outcome

After careful consideration, and taking the above factors into account, the ICO has determined that it is not necessary to proceed with an EN to SCC at this time. Rather, the ICO has decided to issue SCC with a reprimand in accordance with Article 58 of the UK GDPR/Schedule 13(2) of the DPA 2018.

To confirm, this reprimand has been issued in respect of the following infringements of the UK GDPR:

- **Article 5(1)(a) – 'lawfulness, fairness and transparency'**

  This states personal data shall be:

  'processed lawfully, fairly and in a transparent manner in relation to the data subject'

- **Article 5(1)(c) – 'data minimisation'**

  This states that personal data shall be:

  'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'

It is considered that SCC has failed to alleviate the ICO's concerns in respect of its policy for continuous video monitoring when a licensed vehicle is in private use. In particular, the ICO maintains that such use is

neither necessary for, or lawful in respect of, the pursuit of SCC's legitimate aims. Furthermore, SCC has failed to adopt less intrusive alternatives to continuous video recording when a vehicle is in private use; rendering their current processing of personal data in this context excessive.

Further action recommended

Alongside the ICO's decision to issue SCC with a reprimand in this case, the Commissioner also recommends that SCC takes certain steps to improve its compliance with the UK GDPR. In particular:

1. Consider adopting less intrusive alternatives to continuous visual recording when a taxi/PHV is being used for off-duty purposes by a driver.

2. SCC should have a clear policy document and process in place to ensure that drivers are aware of the appropriate circumstances in which the option to audio record is permitted.

   Sufficient driver training should also be provided and refreshed where appropriate.

3. SCC has previously explained to the ICO that there are currently no measures in place for the Council to be notified of faulty vehicle recording/data-bearing devices.

   It was further explained that the frequency of software upgrades for these devices was not regulated.

   It is therefore recommended that SCC review its current policies and procedures to ensure that drivers have working devices that are fit for purpose at all times. In the event that device faults are identified, these should be reported and repaired as soon as possible.

4. Clear and consistent policies should be formed and adhered to by staff in relation to both access to and the security of video and audio footage held by SCC.

   Relevant measures should include:

   - sufficient encryption and/or password protection of vehicle data;

- appropriate storage of data-bearing devices on council premises; and

- the maintenance of accurate, up to date and complete logs of staff access to and downloads of vehicle data.

Reviews of these policies and procedures should be conducted on a periodic basis to ensure that the measures in place are fit for purpose and remain effective for the protection of vehicle data.

5. SCC should review its current retention policies for licensed vehicle recordings to ensure that personal data is only kept for necessary and proportionate time periods in line with storage limitation requirements under the UK GDPR. SCC should also ensure that staff members are fully informed of and consistently adhering to these policies in practice.

6. SCC should ensure that up to date vehicle licensing and data processing agreements are in place between SCC and proprietors/drivers outlining established access and security procedures for in-vehicle recording devices.

   These agreements should also clearly outline the designation of data controllership and processor responsibilities in respect of vehicle recordings.

7. SCC should continue to ensure that fair processing notice stickers placed both inside and outside of licensed vehicles are sufficient to inform individuals of:

   - the nature of data processing taking place;
   - the controller of the data being collected; and
   - where they can find associated privacy information.

   The size and placement of these notices should also be appropriate for sight by all passengers.

8. Finally, in respect of SCC's latest 'Taxi Cameras' Data Protection Impact Assessment (DPIA) of 3 March 2021, we would like to issue the following recommendations:

- SCC should provide further detail on its reasoning for why limousine and contract vehicles are exempt from its continuous recording requirement, based on an assessed low risk.

- SCC should clarify the rationale for its retention of master copies of footage.

- SCC should clarify encryption standards for copies of data held by SCC (on laptops or other media).

- SCC should consider how the right to object would be considered for this data processing more explicitly.

- SCC should consider the publication of its DPIA.

For completeness, we ask that SCC provides a progress update to the ICO on the above recommendations in three months' time, or by no later than **30 September 2022**. Unless otherwise instructed, please provide this update to [redacted]

Whilst the above measures are suggestions, I would like to point out that if further information relating to this incident comes to light, or if any further incidents or complaints of a similar nature are reported to us, we will revisit this matter and formal regulatory action may be considered as a result.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and new powers under the UK GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/about-the%20ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the case closed.

Yours sincerely

[redacted]
Lead Case Officer
Civil Investigations
Regulatory Supervision Service
The Information Commissioner's Office

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the United Kingdom General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes basic details about the complaints, investigations and self-reported data breaches it handles. These details include the name of the organisation concerned, the dates that we opened and closed the case, and the outcome. Examples of published data sets can be found at this link: https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/.

We do not include personal data in the published datasets and will anonymise the names of sole traders etc prior to publication. We also do not publish cases concerning domestic CCTV complaints and may not publish certain other cases if we feel it is not appropriate to do so in the circumstances.

If you wish to raise an objection to us publishing a case in the datasets, whether or not we have published it yet, please contact us explaining your reasons for this at accessicoinformation@ico.org.uk.

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into

consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice.

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Portsmouth City Council
Civic Offices
Guildhall Square
Portsmouth
PO1 2BQ

By email only to: [redacted]

Date: 30 June 2022

Dear [redacted]

Case Reference Number: INV/0509/2020

Thank you for your latest correspondence to the ICO of 20 January 2022. In this, you provided a response to the ICO's further enquiries of 6 December 2021.

I write to inform you that the ICO has now reached a decision in respect of its investigation into INV/0509/2020.

This investigation concerns Portsmouth City Council's (PCC) policy requirement that all licensed taxis, and the majority of private hire vehicles (PHVs), be fitted with a CCTV system that is in permanent operation. This policy results in the continuous recording of all drivers and their passengers in taxis and PHVs licensed by PCC whenever they are in use, to include when that use is for private purposes.

This case has been considered under the United Kingdom General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018 (the DPA 2018) due to the nature of the processing involved. We refer to the UK GDPR and the DPA 2018 together as the 'data protection legislation'.

Our consideration of this case

As you are aware, the ICO previously submitted a Preliminary Enforcement Notice (PEN) to PCC on 4 September 2019. This outlined the Commissioner's intention to issue PCC with an Enforcement Notice (EN) for infringements of Article 5(1)(a) and Article 5(1)(c) of the GDPR.

A further breach of Schedule 1, Part I, Article 8 of the Human Rights Act 1998 was also identified; which in turn amounted to a breach of the fairness requirement of Article 5(1)(a). This is because the latter requires

a balancing exercise which takes into account the justification for the data processing and the potential harmful impact on individuals.

Since issuing its PEN to PCC, representations from PCC in respect of this notice were received on 4 October 2019. A site visit was also undertaken by the ICO's Civil Investigations team, and a series of further enquiries were posed to PCC.

The ICO also wishes to highlight its publication of updated video surveillance guidance in early 2022.

Investigation outcome

After careful consideration, and taking the above factors into account, the ICO has determined that it is not necessary to proceed with an EN to PCC at this time. Rather, the ICO has decided to issue PCC with a reprimand in accordance with Article 58 of the UK GDPR/Schedule 13(2) of the DPA 2018.

To confirm, this reprimand has been issued in respect of the following infringements of the UK GDPR:

- **Article 5(1)(a) – 'lawfulness, fairness and transparency'**

  This states personal data shall be:

  'processed lawfully, fairly and in a transparent manner in relation to the data subject'

- **Article 5(1)(c) – 'data minimisation'**

  This states that personal data shall be:

  'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'

It is considered that PCC has failed to alleviate the ICO's concerns in respect of its policy for continuous video monitoring when a licensed vehicle is in private use. In particular, the ICO maintains that such use is neither necessary for, or lawful in respect of, the pursuit of PCC's legitimate aims. Furthermore, PCC has failed to adopt less intrusive alternatives to continuous video recording when a vehicle is in private

use; rendering its current processing of personal data in this context excessive.

Further action recommended

Alongside the ICO's decision to issue PCC with a reprimand in this case, the Commissioner also recommends that PCC takes certain steps to improve its compliance with the UK GDPR. In particular:

1. Consider adopting less intrusive alternatives to continuous visual recording when a licensed taxi/PHV is being used for off-duty purposes by a driver.

2. PCC has previously explained to the ICO that proprietors have access to footage when requests are made by PCC, or where claims are made against drivers that require further investigation. However, it was emphasised that proprietors should not edit, delete or access footage unless there is a reason to do so.

   Further to this, PCC should ensure that up to date vehicle licensing and data processing agreements are in place between PCC and proprietors/drivers outlining established access and security procedures for in-vehicle recording devices.

   These agreements should also clearly outline the designation of data controllership and processor responsibilities in respect of vehicle recordings.

3. PCC has previously explained to the ICO that in the event that devices malfunction or are no longer working, there is no established requirement for this to be reported to PCC. Upgrades to device software and firmware were also stated to be the responsibility of proprietors.

   Although PCC has referenced its ability to conduct both annual and ad-hoc operational compliance checks on licensed vehicles, these checks do not appear to be undertaken consistently in line with established policies and procedures. Furthermore, insufficient evidence has been provided in respect of steps taken by PCC to ensure that proprietors are adhering to their licensing agreements in respect of regular device inspection and maintenance.

It is therefore recommended that PCC review its current policies and procedures to ensure that drivers have working devices that are fit for purpose at all times. In the event that device faults are identified, these should be reported and repaired as soon as possible.

4. Clear and consistent policies should be formed and adhered to by staff in relation to both access to and the security of vehicle recordings held by PCC.

   Relevant measures should include but are not limited to:

   - sufficient encryption and password protection of vehicle data;
   - appropriate storage of data-bearing devices on council premises; and
   - maintenance of accurate, up to date and complete logs of staff access to and downloads of vehicle data.

   Reviews of these policies and procedures should be conducted on a periodic basis to ensure that the measures in place are fit for purpose and remain effective for the protection of vehicle data.

5. PCC should review its current retention policies for licensed vehicle recordings to ensure that personal data is only kept for necessary and proportionate time periods in line with storage limitation requirements under the UK GDPR. PCC should also ensure that staff members are fully informed of and consistently adhering to these policies in practice.

6. PCC should continue to ensure that fair processing notice stickers placed both inside and outside of licensed vehicles are sufficient to inform individuals of:

   - the nature of data processing taking place;
   - the controller of the data being collected; and
   - where they can find associated privacy information.

   The size and placement of these notices should also be appropriate for sight by all passengers.

7. Finally, in respect of PCC's latest Data Protection Impact Assessment (DPIA) of 18 January 2019 provided to the ICO, we would like to issue the following recommendations:

- PCC should consider the entirety of the processing operation for which it is determining the manner and means of processing.

- PCC should clarify if the data processing undertaken includes location tracking in light of the fact that GPS functionality is a requirement of its technical specification for cameras.

- PCC should revise its template to replace the Privacy Impact Assessment screening questions with a UK GDPR-compliant checklist which considers Article 35(3) and 35(4) requirements.

  See applicable DPIA guidance on the ICO's website.

- PCC should revise its template to ensure necessity and proportionality are considered as required by Article 35(7)(b).

  Any consideration of necessity and proportionality must describe why reasonable alternatives are not possible.

  When relying on public task controllers must evidence the processing is necessary; meaning it is a targeted and proportionate way of achieving the purpose. Other reasonable and less intrusive means of achieving the purpose will likely raise doubts as to the validity of this lawful basis.

  Necessity and proportionality considerations should also evidence compliance with all data protection principles through the lifecycle of the processing.

- PCC should revise its DPIA template to ensure that the likelihood and severity of risk to data subjects is objectively assessed.

  This risk assessment should focus on risks to the rights and freedoms of individuals for all vehicle recordings PCC are the Controller for.

For completeness, we ask that PCC provides a progress update to the ICO on the above recommendations in three months' time, or by no later than **30 September 2022**. Unless otherwise instructed, please provide this update to [redacted]

Whilst the above measures are suggestions, I would like to point out that if further information relating to this incident comes to light, or if any further incidents or complaints of a similar nature are reported to us, we will revisit this matter and formal regulatory action may be considered as a result.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and new powers under the UK GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/about-the%20ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the case closed.

Yours sincerely

[redacted]
Lead Case Officer
Civil Investigations
Regulatory Supervision Service

The Information Commissioner's Office

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the United Kingdom General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes basic details about the complaints, investigations and self-reported data breaches it handles. These details include the name of the organisation concerned, the dates that we opened and closed the case, and the outcome. Examples of published data sets can be found at this link: https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/.

We do not include personal data in the published datasets and will anonymise the names of sole traders etc prior to publication. We also do not publish cases concerning domestic CCTV complaints and may not publish certain other cases if we feel it is not appropriate to do so in the circumstances.

If you wish to raise an objection to us publishing a case in the datasets, whether or not we have published it yet, please contact us explaining your reasons for this at accessicoinformation@ico.org.uk.

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice.

LOQBOX Savings Limited 80
AllState Parkway Henleaze
Business Centre Henleaze,
Bristol
BS9 4PN

By email only to: [redacted] and [redacted]

10 March 2023

Dear [redacted]

Case Reference Number INV/0243/2020

I write to inform you that the Information Commissioner's Office ('ICO') has now completed its investigation into the personal data breach reported by LOQBOX Savings Limited ('LSL') on 22 February 2020.

The case has been considered under the General Data Protection Regulation (the GDPR) due to the nature of the processing involved.

Case Summary

It is my understanding that on 20 February 2020, an unauthorised third party compromised an administrator user account in order to gain access to LSL's systems and exfiltrate customer data. An investigation by LSL was unable to determine how the account was initially compromised, but did identify a lack of IP address lockdown, which meant the database was discoverable from outside LSL's systems.

Data belonging to 250,920 UK Data Subjects was impacted by the incident, with data including names, email addresses and partial card numbers being exposed. LSL confirmed that not all personal data was encrypted at rest, and regular vulnerability scans were not being conducted on the affected systems. LSL also confirmed that the compromised account used to gain unauthorised access was being shared between multiple users.

Our consideration of this case

I have investigated whether LSL has complied with the requirements of data protection legislation.

For more information about our powers under the data protection legislation please see the attached leaflet.

- ICO Enforcement Powers Leaflet – GDPR and DPA 2018

My investigation has found the following issues in relation to the security requirements of the GDPR:

- LSL had not correctly implemented IP address lockdown. NCSC guidance recommends organisations implement allow listing and access controls.[1]

- LSL were allowing multiple users to access the same administrative account. NCSC guidance outlines the risks associated with this practice.[2]

- LSL were not encrypting all data at rest, contrary to best practice. ICO guidance recommends organisations store personal data in an encrypted form to protect against unauthorised access.[3]

- LSL were not conducting regular vulnerability scanning. NCSC guidance recommends regular scanning.[4]

After careful consideration and based on the information provided we have decided to issue LSL with a reprimand in accordance with Article 58 (2) (b) of the GDPR.

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed the GDPR.

- Article 32 (1) which states taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

- Article 32 (1) (b) which states the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including the ability

[1] Common Cyber Attacks: Reducing the Impact – NCSC.GOV.UK
[2] Password Administration for System Owners – NCSC.GOV.UK
[3] Encryption and Data Storage – ICO.org.UK
[4] Vulnerability Scanning Tools and Services – NCSC.GOV.UK

to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

LSL failed to demonstrate that they had appropriate technical and organisational measures in place to ensure a level of security appropriate to the risk. LSL did not follow industry guidelines by allowing shared access to an administrative account, did not implement appropriate IP address lockdown, and were not conducting regular vulnerability scans.

Guidance was available which, had LSL consulted, would have highlighted the steps to take to ensure the security of its systems.

I would like to point out that if further information relating to this subject comes to light, or if any further incidents or complaints are reported to us, we will revisit this matter and further formal regulatory action may be considered as a result.

Further Action Recommended

The Commissioner recommends that LOQBOX Savings Limited should take steps to ensure it is compliant with the GDPR. The information above details the compliance issues relevant to this investigation. The guidance provided in this reprimand should be considered by LOQBOX Savings Limited.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link:

https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest.

We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and powers under the GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link: Communicating our Regulatory and Enforcement Activity Policy (ico.org.uk)

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely

[redacted]

Lead Technical Investigations Officer Tel. [redacted]
Email. [redacted]

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes the outcomes of its investigations. Examples of published data sets can be found at this link (https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice

DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

The Information Commissioner (the Commissioner) issues a reprimand to Nottinghamshire Police in accordance with Schedule 13(2)(c) of the Data Protection Act 2018 (DPA 2018) in respect of certain infringements of the DPA 2018.

The reprimand

The Commissioner has decided to issue a reprimand to Nottinghamshire Police in respect of the following infringements of the DPA 2018:

- Section 40 Data Protection Act 2018 which states that "The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)."

- Section 56 of the Data Protection Act 2018 which states that "Each controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this Part. (2) Where proportionate in relation to the processing, the measures implemented to comply with the duty under subsection (1) must include appropriate data protection policies. (3)The technical and organisational measures implemented under subsection (1) must be reviewed and updated where necessary."

- Section 57(1) of the Data Protection Act 2018 which states that "Each controller must implement appropriate technical and organisational measures which are designed (a) to implement the data protection principles in an effective manner, and (b) to integrate into the processing itself the safeguards necessary for that purpose."

- Section 66(1) of the Data Protection Act 2018 which states that "Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data."

The reasons for the Commissioner's findings are set out below.

The breach in this case was an unauthorised disclosure of the personal data of witnesses via a police officer's unredacted statement on the CPS Digital Case Management system. The evidence has revealed that in this instance, the cause of the disclosure of the personal data of witnesses was the failure to ensure the adequate redaction of the data before disclosing this to the CPS.

The evidence has further revealed that this failure was due to a lack of proper redaction and/or disclosure training. Therefore it would be reasonably foreseeable that there could be officers completing redaction and disclosure without proper training. [redacted]

In addition to this more generally Nottinghamshire Police had no oversight over whether policies regarding redaction and data protection were accessed or understood by officers, instead relying on emails from heads of departments to officers to alert them of any changes in the policy.

Data Protection training was mandatory during induction but there was no oversight over whether this was completed and Nottinghamshire Police are unable to say whether the officers involved in this breach had completed the training. Nottinghamshire Police stated that the completion rate for Data Protection training from 1 December 2020 to 1 December 2022 was 15.85%.

Therefore Nottinghamshire Police failed to ensure appropriate security of the personal data, using appropriate technical or organisational measures in line with Section 40, 56, 57(1) and 66 of DPA18.

Mitigating factors

In the course of our investigation we have noted that human error contributed in part to the breach, there was no actual harm caused to the data subjects or any effect on the outcome of the trial.

Remedial steps taken by Nottinghamshire Police

The Commissioner has also considered and welcomes the remedial steps taken by Nottinghamshire Police in the light of this incident. In particular Nottinghamshire Police worked with the CPS to remove and retrieve the data and steps were taken to ensure the safety of the data subjects affected. It is also noted that in order to prevent a recurrence of the incident Nottinghamshire Police undertook a review of the department's

policies and procedures and will be implementing a SOP in respect of this process. During this process the Information Management Unit (IMU) identified that additional data protection and disclosure guidance would be beneficial to the whole organisation.

Decision to issue a reprimand

Taking into account all the circumstances of this case, including the mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to Nottinghamshire Police in relation to the infringements of sections of the DPA 2018 set out above.

Further Action Recommended

The Commissioner recommends that Nottinghamshire Police should take certain steps to ensure its compliance with DPA 2018. With particular reference to section 40 of the DPA 2018, the following steps are recommended:

1. Consider providing explicit redaction training to employees involved in the disclosure or redaction of evidence.

2. Review data protection training schedules and systems to ensure that adequate monitoring is in place in order to improve levels of compliance and completion.

3. Consider incorporating anonymised examples of incidents into data protection training to raise awareness of the potential for breaches to occur, with particular attention being given to their inclusion in departments where such incidents have occurred.

4. Ensure that the collective learnings from data breaches are shared across the whole force, particularly if the type of processing is common across areas.

5. Complete the implementation of the Standard Operating Procedure, dissemination of guidance and mandatory NCALT Data Protection Training.

Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Travel Healthcare Insurance Solutions Inc
80 AllState Parkway
Markham, Ontario
Canada
L3R 6H3

By email only to: [redacted]

17 October 2022

Dear [redacted]

Case Reference Number INV/0916/2021

I write to inform you that the Information Commissioner's Office ('ICO') has now completed its investigation into the personal data breach reported by Travel Healthcare Insurance Solutions Inc ('THIS') on 03 July 2021.

The case has been considered under the General Data Protection Regulation (the GDPR) due to the nature of the processing involved.

Case Summary

It is my understanding that on 19 June 2021, an unauthorised third party [redacted] to gain access to, and delete, [redacted] databases within THIS' systems. The databases contained the personal data of [redacted] UK Data Subjects, and included data relating to [redacted] An investigation by THIS found that the [redacted] used to gain access had been first compromised by a previously reported [redacted] attack on 12 May 2021.

Although THIS confirmed that after the May incident a penetration test and static code analysis was carried out to determine that the [redacted] vulnerability was no longer present, they advised that whilst the [redacted] compromised in the incident were intended to be [redacted], this had not yet been completed by 19 June 2021.

Our consideration of this case

I have investigated whether THIS has complied with the requirements of data protection legislation.

For more information about our powers under the data protection legislation please see the attached leaflet.

- ICO Enforcement Powers Leaflet – GDPR and DPA 2018

My investigation has found the following issues in relation to the security requirements of the GDPR:

- THIS did not [redacted] known [redacted] in a timely manner. The NIST incident response framework outlines the steps to take when recovering from a cyber incident.[1] The NCSC also recommends [redacted] when recovering from an incident.[2]

After careful consideration and based on the information provided we have decided to issue THIS with a reprimand in accordance with Article 58 (2) (b) of the GDPR.

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed the GDPR.

- Article 32 (1) which states taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

This incident may have been avoided if THIS had [redacted] THIS had themselves recognised the need to [redacted] after the May incident, however, they did not act quickly enough to remediate the issue.

The affected [redacted] was a [redacted], resetting the [redacted] for such an [redacted] would have taken THIS a [redacted], as [redacted] is a quick and simple task. As THIS had remedied the [redacted] vulnerability, the only other way to access the database was with the [redacted] obtained in the May attack. Had the [redacted] been [redacted] promptly, the June incident would not have occurred, as the [redacted]

[1] NIST incident response framework – National Institute of Standards and Technology
[2] Small Business Guide: Response & Recovery – NCSC.GOV.UK

Guidance was available which, had THIS consulted, would have highlighted the steps to take to ensure the security of its systems. This includes the NCSC's incident response checklist. Microsoft also provides guidance on recovering from cyber incidents, had THIS consulted these guides, it is likely their systems would have been secured appropriately.

I would like to point out that if further information relating to this subject comes to light, or if any further incidents or complaints are reported to us, we will revisit this matter and further formal regulatory action may be considered as a result.

Further Action Recommended

The Commissioner recommends that Travel Healthcare Insurance Solutions Inc should take steps to ensure it is compliant with the GDPR. The information above details the compliance issues relevant to this investigation. The guidance provided in this reprimand should be considered by Travel Healthcare Insurance Solutions Inc.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link:

https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and powers under the GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Information Commissioner's Office

Yours sincerely

[redacted]

Lead Technical Investigations Officer
Tel. [redacted]
Email. [redacted]

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes the outcomes of its investigations. Examples of published data sets can be found at this link (https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice

DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: Hull University Teaching Hospitals NHS Trust

OF: Castle Hill Hospital, Castle Road, Cottingham, HU16 5JQ

The Information Commissioner (the Commissioner) issues a reprimand to Hull University Teaching Hospitals NHS Trust (the Trust) in accordance with Article 58 (2)(b) of the UK General Data Protection Regulation in respect of certain infringements of the UK GDPR.

In summary, on 15 July 2020 the Trust made an alteration to its electronic patient record system (the system update) to allow clinic letters to be automatically sent to a patient's General Practitioner (GP) electronically if generated within the system. Specifically, when clinic letter templates on the system with a 'SR' prefix in the title were used, they would be automatically sent to a patient's GP, and those without the prefix would not.

Clinical correspondence between a hospital specialist who has seen a patient in an [redacted] clinic and the patient's GP typically contains information regarding the consultation and any relevant clinical findings. Clinic letters are sent after every clinic appointment at the hospital, for every patient, to the relevant GP Practice and the patient. Clinic letters contain personal data including special category data in the form of health data as defined by Article 9 (1) of the UK GDPR ie data relating to healthcare, diagnosis, treatments, and future follow up plans.

The Trust provides [redacted] for patients [redacted] and in respect of [redacted], patients can request that [redacted] does not contact their GP or notify their GP of their [redacted] records patients' communication preferences regarding clinical correspondence which are consulted by [redacted] prior to sending clinic letters.

Following the system update, between 15 July 2020 and November 2021 [redacted] used clinic letter templates on the system which included the 'SR' prefix in error [redacted] for patients who had opted for their GPs not to receive correspondence. This resulted in 40 patients' clinic letters, up to 60 clinic letters in total, being sent to affected patients' GPs against their request.

Information obtained as part of the ICO's investigation shows evidence that distress has been caused to some affected patients due to the

disclosure of this information to their GP Practice. For example, in some instances, [redacted]

Further to the above, during the Trust's investigation into this matter, the Trust identified that it needed to look at other areas of the Trust [redacted], as some had referred to a [redacted] in their clinic letter to the GP.

The reprimand

The Commissioner has decided to issue a reprimand to Hull University Teaching Hospitals NHS Trust in respect of the following infringements of the UK GDPR:

- Article 5 (1)(f) which states personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

- Article 25 (1) which states "…the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures…"

- Article 32 (1) which states "…the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…"

The reasons for the Commissioner's findings are set out below.

Article 25 (1) of the UK GDPR

The ICO understands that the work relating to the system update was carried out within [redacted] and in conjunction with [redacted] of [redacted] and documentation regarding this process has been provided to the ICO.

However, staff within [redacted] were not consulted during the development of the system update and no risk assessment was undertaken, as the Trust considered it was a minor amendment to the system to automate the process of sending clinic letters to GPs.

The ICO considers the above resulted in an infringement of Article 25 (1) of the UK GDPR.

Articles 5 (1)(f) and 32 (1) of the UK GDPR

The Trust confirmed that prior to the system update, [redacted] was communicated to by the [redacted] and [redacted] via email. The Trust said "…staff were given a clear instruction on which templates to use for automated and non-automated clinic letters". However, although instructions provided to staff in July 2020 and April 2021 stated that letters that included the 'SR' prefix would go electronically to the GP and provided a contact for any staff queries, the instructions were written in a way that assumed all clinic letters were required to be sent to a patient's GP and not to use any other templates.

Additionally, no specific guidance was provided to [redacted] regarding the system update as the Trust confirmed it was a whole Trust instruction. The Trust confirmed it is up to [redacted] to take the updates and instructions provided by the [redacted] and the [redacted] and implement changes in their department as necessary. The ICO understands that [redacted] had not realised that the system update would impact the internal team processes in place.

[redacted] assumed that if they did not put a patient's GP details into the letter or typed 'Not for sending to GP' the system would not automatically send it, but rather store it in the patient record. However, the system update meant that the clinic letter would be automatically sent to the GP registered on the patient's electronic record, it was not dependent on the content of the letter. The Trust also confirmed that [redacted] had "…continued to use the template that had now become automated rather than the template that had not become automated in the system."

Further to the above, there was no training delivered in respect of the system update to [redacted] staff as the Trust did not consider it necessary, this is because the functionality was already in use and being used by others, but the range of templates that could be sent to GPs was extended.

Therefore, the ICO considers the Trust did not implement appropriate technical and organisational measures to ensure the security of the personal data involved. As a result, personal data was shared with affected patients' GPs against their request, which resulted in infringements of Articles 5 (1)(f) and 32 (1) of the UK GDPR.

Other points of note

During its investigation, the ICO has identified that there is a delay in reporting this matter to the ICO. The Trust confirmed due to the nature of the incident, it took time to ascertain the full extent of the incident, but the delay was also because of human error. Additionally, on some occasions during the ICO's investigation, the Trust did not provide a response, or, a full response within the timeframe provided by the ICO.

Remedial steps taken by the Trust

The Commissioner has also considered the remedial steps taken by the Trust in the light of this matter.

In summary, a specific letter template was created within the system for [redacted] to use going forward, to avoid confusion, which would not automatically be sent to patients' GPs.

The Trust has taken steps in an attempt to notify affected data subjects of this matter and to provide them with the option for the Trust to contact their GP and request removal of the clinic letters from their systems. The Trust confirmed to the ICO that all GPs for patients who requested removal had been contacted and this was in progress during the ICO's investigation.

The [redacted] have received further training and since this matter occurred, the Trust is conducting face to face data protection training in teams as well as arranging weekly sessions that staff can enrol onto.

Further to the above, the Trust's recommendations to the [redacted] were to ensure any communications about system changes that affect their services include provision for teams to raise any questions or concerns that can be fed back to the [redacted], and when system changes occur, ensure that the staff working in [redacted] are aware of the potential implications and what they are required to do. This may include teams having allotted time with the [redacted] before the changes are implemented. The ICO understands for a recent major change, the [redacted] spent time on wards and departments at various times.

Finally, the Trust was looking into a solution regarding its identification of other areas of the Trust that had referred to a [redacted] in their clinic letter to the GP.

Decision to issue a reprimand

Taking into account all the circumstances of this case including the remedial steps, the Commissioner has decided to issue a reprimand to

Hull University Teaching Hospitals NHS Trust in relation to the infringements of Article 5 (1)(f), Article 25 (1) and Article 32 (1) of the UK GDPR set out above.

Further Action Recommended

The Commissioner recommends that Hull University Teaching Hospitals NHS Trust should take certain steps to ensure its compliance with the UK GDPR. With particular reference to Article 5 (1)(f), Article 25 (1) and Article 32 (1) of the UK GDPR unless otherwise specified, the following steps are recommended. The Trust should:

1. Follow up on and conclude all enquiries to all affected patients' GP practices to request and confirm removal of any personal data sent in error, where this has been requested by the affected patient.

2. Consider introducing a solution or approach to ensure preferences provided to the patient regarding clinical correspondence are understood by all areas of the Trust where appropriate, meaning personal data is not shared onward by any other area of the Trust against a patient's request.

3. Prior to implementing any system updates, such as the system update concerned in this matter, the Trust should ensure that:

    3.1 A risk assessment is undertaken.
    3.2 Measures such as those put in place for recent major changes take place. Specifically, ensuring the [redacted] spends time with relevant departments to make staff aware of changes and conduct training where necessary.
    3.3 Explicit instructions are issued to ensure that all relevant staff understand the impact of the change and considers how this may affect their team's processes.

4. Implement further measures within the Information Governance Team responsible for assessing and reporting personal data breaches to the ICO in order to:

    4.1 Ensure that all enquiries received in any future investigations conducted by the ICO, if applicable, are responded to fully in line with the deadlines set by the ICO. Where the Trust is unable to adhere to these deadlines, the ICO should be contacted without delay and before the deadline set to discuss any extensions required.
    4.2 Ensure that all personal data breaches are reported to the ICO in line with Article 33 of the UK GDPR.

Hull University Teaching Hospitals NHS Trust should provide a progress update on the above recommendations within six months of the date of this reprimand, ie by **17 February 2024**.