Case reference

IC-31191-G5C6

Information Commissioner's Office

From:	Jade.Choudhury@ico.org.uk
To:	icocasework@ico.org.uk;
CC:	
Subject:	INITIAL BREACH REPORT - Triaged CY - RFI - Personal data breach notification - IC-31191-G5C6
Direction:	Incoming
Date Received:	23/12/2019 11:12

From: Data Compliance [mailto:data.compliance@Justice.gov.uk]
Sent: 20 December 2019 18:16
To: casework <casework@ico.org.uk>
Cc: Data Compliance <data.compliance@Justice.gov.uk>; [redacted]
Subject: JC INITIAL BREACH REPORT - Triaged CY - RFI - Personal data breach notification

External: This email originated outside the ICO.

Dear Colleagues,

Please find attached, a 'self-report' form, relating to a data breach involving personal data for which the Ministry of Justice, is the data controller.

Ministry of Justice [redacted]
Ministry of Justice
Data Protection & GDPR Compliance Advisor
Data Protection Team
Digital and Technology Directorate
3rd floor, 10 South Colonnade, Canary Wharf, E14 4PU
Telephone: [redacted]
Follow us on Twitter @MoJGovUK

Protecting and advancing the principles of justice

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. Please do not include any of the personal data involved in the breach when completing this form. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

If you have already spoken to a member of ICO staff about this breach, please give their name:

N/A

Report type

Initial report

Follow-up report

(Follow-up reports only) ICO case reference: N/A

Reason for report – after consulting the guidance

I consider the incident meets the threshold to report

I do not consider the incident meets the threshold to report, however I want you to be aware

I am unclear whether the incident meets the threshold to report

About the breach

What has happened?

Tell us as much as you can about what happened, what went wrong and how it happened.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Was the breach caused by a cyber incident?

[redacted]

How did you find out about the breach?

[redacted]

[redacted]

When did you discover the breach?

Date: 18 December 2019

Time: 16:42

When did the breach happen?

Date: 7 December 2019

Time:

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data
- ☒ Basic personal identifiers, eg name, contact details
- ☒ Identification data, eg usernames, passwords
- ☐ Economic and financial data, eg credit card numbers, bank details
- ☐ Official documents, eg driving licences
- ☐ Location data
- ☐ Genetic or biometric data
- ☐ Criminal convictions, offences
- ☐ Not yet known
- ☒ Other (please give details below)

National Insurance Number

Number of personal data records concerned?

Total: 121,109
Of that total, 48,740 contain National Insurance number

How many data subjects could be affected?

121,109

Categories of data subjects affected (tick all that apply)

- ☒ Employees
- ☐ Users
- ☐ Subscribers
- ☐ Students
- ☐ Customers or prospective customers
- ☐ Patients
- ☐ Children
- ☐ Vulnerable adults
- ☐ Not yet known
- ☐ Other (please give details below)

Potential consequences of the breach

Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to data subjects

At this stage, we assess the likelihood of detriment materialising to be low. We will review this position as our investigations continue and further information comes to light.

MoJ are not aware that any actual harm to data subjects has materialised.

What is the likelihood that data subjects will experience significant consequences as a result of the breach?

- Very likely
- Likely
- Neutral - neither likely nor unlikely
- Unlikely
- Very unlikely
- Not yet known

Please give details

[redacted]

(Cyber incidents only) Has the confidentiality, integrity and/or availability of your information systems been affected?

[redacted]

(Cyber incidents only) If you answered yes, please specify (tick all that apply)

[redacted]

(Cyber incidents only) Impact on your organisation

[redacted]

(Cyber incidents only) Recovery time

[redacted]

Had the staff member involved in this breach received data protection training in the last two years?

Yes

No

Don't know

(Initial reports only) If there has been a delay in reporting this breach, please explain why

The cause of the delay in the sub-processor notifying the data processor and in turn the MoJ, is as yet undetermined. We are investigating the reasons for this delay and will cover this aspect more fully in our follow-up report.

(Follow-up reports only) Describe any measures you had in place before the breach with the aim of preventing a breach of this nature*

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, eg confirmed data sent in error has been destroyed, updated passwords, planning information security training.

[redacted]

(Follow-up reports only) Outline any steps you are taking to prevent a recurrence, and when you expect they will be completed*

Have you told data subjects about the breach?

Yes, we've told affected data subjects

We're about to, or are in the process of telling data subjects

No, they're already aware

No, but we're planning to

No, we've decided not to

We haven't decided yet if we will tell them or not

Something else (please give details below)

We are publishing a general message on the MoJ intranet to inform all staff potentially affected by this breach. At this stage, we have not contacted individual data subjects directly and will continue to review this as further details come to light.

Have you told, or are you planning to tell any other organisations about the breach?

eg the police, other regulators or supervisory authorities. In case we need to make contact with other agencies

If you answered yes, please specify

Cabinet Office, Government Shared Services and MoJ Departmental Trade Unions

About you

Organisation (data controller) name

Ministry of Justice

Registered organisation address

102 Petty France, London SW1H 9AJ

Person making this report

In case we need to contact you about this report

Name: [redacted]

Email: data.compliance@justice.gov.uk

Phone: [redacted]

Data protection officer

Or the senior person responsible for data protection in your organisation

☐ Same details as above

Name: Amie Alekna

Email: amie.alekna@justice.gov.uk

Phone: [redacted]

Sending this form

Initial report
If this is your initial report, please send your completed form to casework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report
If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

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

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number. If we consider the incident is minor or you have indicated that you do not consider it meets the threshold for reporting, you may not receive a response from us.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.

From: icocasework@ico.org.uk
To: data.compliance@Justice.gov.uk;
CC:
Subject: Acknowledgement - IC-31191-G5C6
Direction: Outgoing
Date Sent: 23/12/2019 11:23

Reference Number IC-31191-G5C6

Dear [redacted]

Thank you for contacting the ICO to report a personal data breach. The breach was reported to the ICO on 20 December 2019.

The ICO will use the information you have provided to determine what course of action is necessary. We shall contact you in due course to confirm the outcome.

In the meantime, we would recommend that you read the security guidance on our website.

If you would like to provide any additional information about the incident reported, please send it to icocasework@ico.org.uk and enter the reference number in the subject line. This will ensure the correspondence is added directly to the correct electronic case file.

If the person we should contact about this case changes, please let us know.

If we can be of any further assistance please contact our Helpline on 0303 123 1113.

Yours sincerely

Jade Choudhury

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 ico.org.uk twitter.com/iconews
Please consider the environment before printing this email

From: data.compliance@justice.gov.uk
To: icocasework@ico.org.uk;
CC: data.compliance@justice.gov.uk;
Subject: RE: Acknowledgement - IC-31191-G5C6
Direction: Incoming
Date Received: 31/12/2019 20:02

External: This email originated outside the ICO.
Dear Ms Choudhury,

On behalf of the Ministry of Justice, I now attach an up-dating report, in respect of data incident IC-31191-G5C6.

Ministry of Justice [redacted]
Ministry of Justice
Data Protection & GDPR Compliance Advisor
Data Protection Team
Digital and Technology Directorate
3rd floor, 10 South Colonnade, Canary Wharf, E14 4PU
Telephone: [redacted]
Follow us on Twitter @MoJGovUK

Protecting and advancing the principles of justice

From: ICO Casework [mailto:icocasework@ico.org.uk]
Sent: 23 December 2019 11:23
To: Data Compliance <data.compliance@Justice.gov.uk>
Subject: Acknowledgement - IC-31191-G5C6

Reference Number IC-31191-G5C6

Dear [redacted]

Thank you for contacting the ICO to report a personal data breach. The breach was reported to the ICO on 20 December 2019.

The ICO will use the information you have provided to determine what course of action is necessary. We shall contact you in due course to confirm the outcome.

In the meantime, we would recommend that you read the security guidance on our website.

If you would like to provide any additional information about the incident reported, please send it to icocasework@ico.org.uk and enter the reference number in the subject line. This will ensure the correspondence is added directly to the correct electronic case file.

If the person we should contact about this case changes, please let us know.

If we can be of any further assistance please contact our Helpline on 0303 123 1113.

Yours sincerely

Jade Choudhury

Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 ico.org.uk twitter.com/iconews
Please consider the environment before printing this email

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. Please do not include any of the personal data involved in the breach when completing this form. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

If you have already spoken to a member of ICO staff about this breach, please give their name:

N/A

Report type

Initial report

◉ Follow-up report

(Follow-up reports only) ICO case reference: IC-31191-G5C6

Reason for report – after consulting the guidance

◉ I consider the incident meets the threshold to report

I do not consider the incident meets the threshold to report, however I want you to be aware

I am unclear whether the incident meets the threshold to report

About the breach

What has happened?

Tell us as much as you can about what happened, what went wrong and how it happened.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Was the breach caused by a cyber incident?

[redacted]

How did you find out about the breach?

[redacted]

[redacted]

[redacted]

When did you discover the breach?

Date: 18 December 2019

Time:

When did the breach happen?

Date: 7 December 2019

Time:

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data
- ☒ Basic personal identifiers, eg name, contact details
- ☒ Identification data, eg usernames, passwords
- ☐ Economic and financial data, eg credit card numbers, bank details
- ☐ Official documents, eg driving licences
- ☐ Location data
- ☐ Genetic or biometric data
- ☐ Criminal convictions, offences
- ☐ Not yet known
- ☒ Other (please give details below)

National Insurance Number, individual training records

Number of personal data records concerned?

Total: 121,109
Of that total, 48,740 contain National Insurance number

How many data subjects could be affected?

121,109

Categories of data subjects affected (tick all that apply)

- ☒ Employees
- ☐ Users
- ☐ Subscribers
- ☐ Students
- ☐ Customers or prospective customers
- ☐ Patients
- ☐ Children
- ☐ Vulnerable adults
- ☐ Not yet known
- ☒ Other (please give details below)

Former MoJ employees and employees of some third party organisations

Potential consequences of the breach

Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to data subjects

At this stage, we assess the possible impact on data subjects to be low. We will continue to review this position as our investigations continue.

MoJ are not aware that any actual harm to data subjects has materialised.

What is the likelihood that data subjects will experience significant consequences as a result of the breach?

Very likely

Likely

Neutral - neither likely nor unlikely

◉ Unlikely

Very unlikely

Not yet known

Please give details

We currently assess the likelihood of significant consequences materialising to be low. [redacted]

We will continue to review this position as our investigations continue.

(Cyber incidents only) Has the confidentiality, integrity and/or availability of your information systems been affected?

[redacted]

(Cyber incidents only) If you answered yes, please specify (tick all that apply)

[redacted]

(Cyber incidents only) Impact on your organisation

[redacted]

(Cyber incidents only) Recovery time

Had the staff member involved in this breach received data protection training in the last two years?

- Yes
- No
- (•) Don't know

(Initial reports only) If there has been a delay in reporting this breach, please explain why

(Follow-up reports only) Describe any measures you had in place before the breach with the aim of preventing a breach of this nature*

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, eg confirmed data sent in error has been destroyed, updated passwords, planning information security training.

[redacted]

As soon as the MoJ Data Protection Officer was made aware of the breach, a Data Breach Management Team was mobilised, in line with incident handling protocols. The Data Breach Management Team has held daily meetings to track progress of the investigation.

Concurrently, robust investigations by MoJ technical specialists were initiated to determine the full extent of the breach. This investiagtion is continuing.

An important part of our investigation has been the assessment of risks associated with the breach, particularly the assessment of potential adverse consequences for data subjects and the likelihood of such circumstances materialising. As we continue to gain greater insight into the extent of the personal data involved, we will continue to assess the potential for, and likelihood of, detriment.

The MoJ has set procedures for managing data breaches, which are reviewed on a regular basis. We plan to review the effectiveness of our response to this particular incident, in order to continuously improve our data breach management response.

(Follow-up reports only) Outline any steps you are taking to prevent a recurrence, and when you expect they will be completed*

[redacted]

[redacted]

Have you told data subjects about the breach?

◉ Yes, we've told affected data subjects

We're about to, or are in the process of telling data subjects

No, they're already aware

No, but we're planning to

No, we've decided not to

We haven't decided yet if we will tell them or not

Something else (please give details below)

We have published, and continue to update, a message for all MoJ employees on the intranet. We have encouraged vigilance online and warned of the possibility of phishing emails or other unusual approaches.

[redacted]

Have you told, or are you planning to tell any other organisations about the breach?

eg the police, other regulators or supervisory authorities. In case we need to make contact with other agencies

If you answered yes, please specify

Cabinet Office, Government Shared Services, National Cyber Security Centre, MoJ Departmental Trade Unions and third party organisations whose employees are affected.

About you

Organisation (data controller) name

Ministry of Justice

Registered organisation address

102 Petty France, London SW1H 9AJ

Person making this report

In case we need to contact you about this report

Name: [redacted]

Email: data.compliance@justice.gov.uk

Phone: [redacted]

Data protection officer

Or the senior person responsible for data protection in your organisation

☐ Same details as above

Name: Amie Alekna

Email: amie.alekna@justice.gov.uk

Phone: [redacted]

Sending this form

Initial report
If this is your initial report, please send your completed form to casework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report
If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

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

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number. If we consider the incident is minor or you have indicated that you do not consider it meets the threshold for reporting, you may not receive a response from us.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.

From: icocasework@ico.org.uk
To: data.compliance@Justice.gov.uk;
CC:
Subject: ICO Decision - IC-31191-G5C6
Direction: Outgoing
Date Sent: 14/01/2020 15:47

Reference Number IC-31191-G5C6

Dear [redacted]

I am writing further to your personal data breach report of 20 December 2019 and additional information you have provided on 31 December 2019 regarding [redacted] leading to the unintended exposure of personal information, affecting up to 121,109 data subjects.

Thank you for the information you have provided.

Data Security Requirements

You are required to have appropriate technical and organisational measures in place to ensure the security of personal data.

Our Decision

We have considered the information you have provided and we have decided that no further action by the ICO is necessary on this occasion. This decision is based on the information we have recorded about the breach. If you believe that any of the information we have recorded is incorrect you should tell us as soon as possible.

The reasons for our decision are as follows:

- This appears to have been an isolated incident [redacted]
- Whilst this data breach may have affected a large number of data subjects, the actual sensitivity of the personal data involved in this breach appears to be low;
- [redacted] you have received no evidence to suggest that the breach has resulted in any detriment to the data subjects;
- In addition, you consider it to be unlikely that the personal data breach would result in a risk to the rights and freedoms of any data subjects and are continuing to investigate any future risks that may occur;
- Your organisation have taken action in response to the incident [redacted]

However, we recommend that you continue to review the causes of this incident to ensure that you understand how and why it occurred, and what steps you need to take to prevent it from happening again.

In particular, we recommend that you:

- Consider the preventative measures you had in place prior to this incident and establish whether these processes had been followed. You may need to consider whether or not these measures were appropriate in this instance and if increased security measures may need to be implemented;
- Continue to monitor any potential risks or detriment to the data subjects as a result of this incident and take action to mitigate any risks that you may become aware of. If you were to find out further information that changes your risk assessment you should take immediate action to address this development and let the ICO know at the earliest opportunity.

Please note that as a result of a breach an organisation may experience a higher volume of information rights requests and complaints, particularly in relation to access and erasure. If you receive these complaints, you should have a contingency plan, such as extra resources, to deal with these complaints. You should not refer these complaints to the ICO as a matter of course, and it is important that you continue to deal with complaints, alongside the other work that has been generated as a result of the breach.

Please also note that we may make additional enquiries if we become aware of new information which affects the circumstances of this case.

Thank you for reporting the incident. Further information and guidance relating to data security is available on our website at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

We now consider the matter to be closed.

Yours sincerely

Christopher Yost
Lead Case Officer
0330 414 6474

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 ico.org.uk twitter.com/iconews
Please consider the environment before printing this email