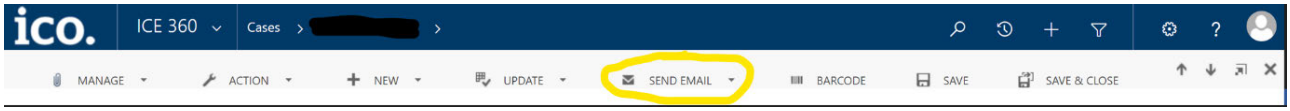
Criminal offences relating to personal data are defined under s170 – s173 DPA 2018 inclusive.

This process should be followed for cases where it appears that data has been taken or retained unlawfully, deleted to prevent it being served in response to a SAR, or deliberately had redacted material re-exposed.

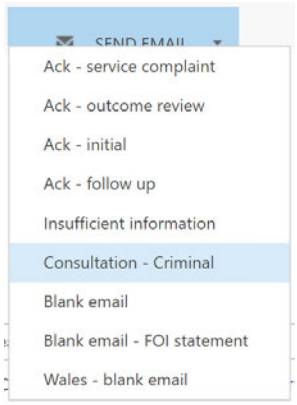
Written reports:

First set up the case following the usual **ICE – Case set ups** process. If there is an s170 element (as outlined above) then the case will need to be referred to CRIT for a decision on whether they will investigate further.

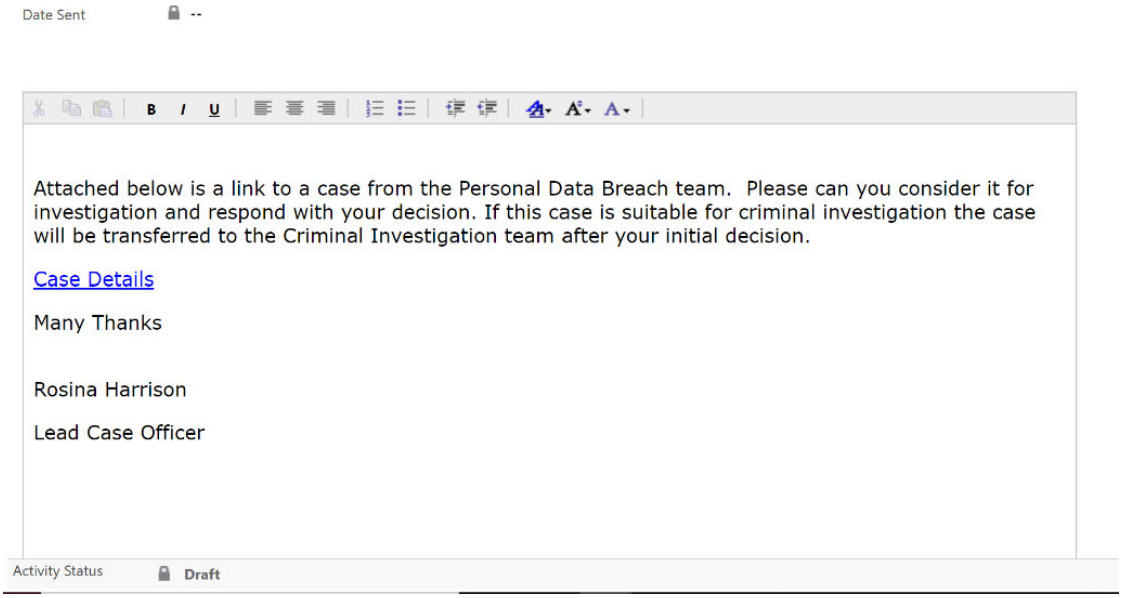
Sending a CRIT consult
You can send a CRIT consult by selecting the "Send Email" option from the toolbar on the ICE case



and then choosing "Consultation – Criminal" from the drop down menu.



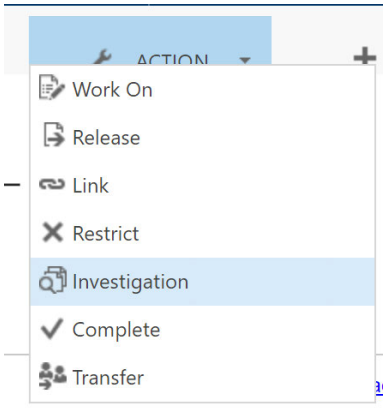
This will auto-generate an email from the case, which should be sent to Criminal Investigations.



CRIT response: Investigation pursued

If the Criminal Investigation Team respond to say that they want to conduct a further investigation (usually they will say 'Crimson case created') then you should ensure that the ICE breach report is completed and choose "Criminal investigation pursued" from the Further investigation required dropdown.

The case status should be amended to "Investigation" via the Action tab from the ribbon at the top of the case page.



The case should finally be transferred to the Criminal Investigations queue. This is done via "Queues", "Cases I am working on", add a tick next to the case in question. Select "Transfer" and choose "Criminal Investigation".

CRIT response: NFA

If, however, the Criminal Investigation Team respond to say that they do not wish to take the case for further investigation (usually they say NFA – no further action) then process the case in accordance with their advice, reviewing the data controller's technical and organisational measures as you would with any other self-reported breach.

You should review the case to establish whether there is sufficient information on which a judgement can be made from the perspective of the PDB team looking at the security breach. If further information is required to make this assessment, you may need to send an RFI.

If further information is received from the organisation you should send another CRIT consult as the information may impact CRIT's decision to pursue an investigation.

The s170 letters process map should be used to help you decide which letter to use when closing a s170 case.

Telephone reports:

When receiving a potential s.170 by telephone, set up the case and complete the test email and send the acknowledgement with rendition as normal. Obtain and record as much information as possible, particularly in respect of any evidence that the personal data was obtained and/or retained unlawfully, and the potential detriment to any data subjects.

Explain to the data controller that this is a two tier process. We will look at:

1. The alleged perpetrator of the potential offence of unlawfully taking/ retaining data. An assessment will be carried out by the Criminal Investigation Team, who will decide whether to proceed in accordance with the Regulatory Action Policy. This decision will look at:

a. Is there sufficient evidence to support a prosecution in this case?
b. Is it in the public interest to prosecute this case?

2. The data controller's technical and organisational measures to protect the personal data they control and process.

We receive many reports of incidents where a former employee has taken client data because they are setting up their own business or are working for a rival company. These cases will be assessed in the usual way, but it may be helpful to manage the expectations of the data controller in the initial phone call: make it clear that the main purpose of the Data Protection Act 2018 is to protect the rights of individuals in respect of personal information which relates to them, not to protect the commercial interests of organisations who hold that information. It is not the ICO's policy to pursue 'business to business' matters where little or no detriment has been caused to data subjects. In most cases, unwanted contact for marketing purposes is unlikely to cause significant detriment beyond annoyance.

It may be helpful to explain that the ICO has limited resources and therefore needs to be selective with regard to the cases it can prosecute. Decisions are made in accordance with the ICO's Regulatory Action Policy, a copy of which is available on the website.

Cases brought under s.170 – 173 of the DPA 2018 are heard in the Criminal Court and have to be proven to the criminal standard, i.e. beyond all reasonable doubt. Individuals may seek to bring private prosecutions, but these would have to be proven to the same standard and the authority of the ICO or the DPP would be required before the matter could be brought before the courts (s.197 DPA 2018).

An individual can commence a civil action, which would be to the civil burden of proof i.e. on the balance of probabilities, a lower burden than the criminal burden. Anyone seeking to do this should be advised to obtain independent legal advice.

Information required when assessing a potential criminal offence under the DPA 2018:

- What is the nature of the personal information that has been unlawfully obtained?
- When was it obtained?
- How was it obtained?
- What information has been received regarding the motive behind the incident?
- Did the individual obtaining the personal information know that their action was unlawful or were they reckless in respect of this?
- Are there any witnesses to the personal information being obtained, or other evidence such as an electronic audit trail?

- Has the person suspected of obtaining the personal data provided any verbal or written explanation of their action? If so, where is this recorded?
- Has a disciplinary investigation been commenced? If so, what was the outcome of this? Can they provide a copy of the investigation report?
- Did the person suspected of obtaining the data have legitimate access to the information at the time it was obtained?
- Has the personal information been used since being obtained? What for?
- Has there been any detriment for the data subjects as a result of the incident?
- Where is the personal data now? Has it been recovered?
- Has the data controller requested that the data be returned or destroyed? What was the response?
- Has this matter been referred to any other law enforcement agency or regulator?
- Have any legal proceedings been commenced?

Offence of retaining personal data without the consent of the data controller:

We receive many reports where data may have been obtained lawfully, e.g. the recipient of the data may have received it in error following a personal data breach by the data controller, or may have had legitimate access to the data at the time it was initially obtained, but the recipient then retains it against the data controller's wishes. These cases should be referred to CRIT in the usual way, but please be aware of the following advice that CRIT have provided:

1. **Personal Data <u>unlawfully</u> obtained prior to 25 May 2018 (pre-GDPR) and unlawfully retained post-GDPR** relates to any data retained by the person(s) alleged to have unlawfully obtained it - this may be investigated subject to there being sufficient evidence to substantiate the allegation and whether it was in line with the Regulatory Action Policy. NB – the unlawful obtaining would be investigated as a s. 55 DPA 1998 offence.
2. **Personal Data <u>lawfully</u> obtained prior to 25 May 2018 (pre-GDPR) and unlawfully retained post-GDPR** relates to any data lawfully obtained by a person and then retained without the consent of the controller. We would need clear evidence that the defendant was aware, or ought to have been aware, after the 2018 Act came in, that the retention was not consented to by the Controller. For example, it

was clear in the employment terms & conditions or contract that retaining of personal data was contrary to the Controller's internal policy and ideally there is evidence that the Controller has requested the return of the data putting the person on notice that the retention was not consented to. Therefore, Controllers should write and warn ex-employees that if they continue to retain the data in question they could be committing an offence. If they have had such a warning and continue to retain, but the original data was obtained pre-2018 Act, it could be a s170 offence. This may be investigated subject to there being sufficient evidence to substantiate the allegation and whether it was in line with the Regulatory Action Policy.

3. **Personal Data <u>unlawfully</u> obtained on or after 25 May 2018 (post-GDPR) and unlawfully retained** thereafter relates to any data retained by the person(s) alleged to have unlawfully obtained it - this may be investigated subject to there being sufficient evidence to substantiate the allegation and whether it was in line with the Regulatory Action Policy.
4. **Personal Data <u>lawfully</u> obtained on or after 25 May 2018 (post-GDPR) and unlawfully retained** thereafter relates to any data lawfully obtained by a person and then retained without the consent of the controller. The Controller ideally has to provide evidence that they have requested return of the data as outlined at point 2 or the Controller has clear policies that set out that there is no consent for retaining in certain circumstances that also puts the person on notice – e.g. that upon leaving employment any data still held would not be retained with their consent. This may be investigated subject to there being sufficient evidence to substantiate the allegation and whether it was in line with the Regulatory Action Policy.

If an individual has obtained personal data as a result of a personal data breach, and wishes to retain it as proof of the breach or evidence in other proceedings, they should be advised that this data must be returned or disposed of. The recipient of the data can request written confirmation from the data controller that material was disclosed in error, but the personal data itself should be destroyed or returned as directed by the DC. Under no circumstances should the recipient be advised to retain the data.

Version	Changes made	Date	Made By
0.1	First Draft	11 October 2022	Rosina Harrison
0.11	Uploaded onto SharePoint and Links checked.	3 April 2023	Sophie Judge

Approach to s170 letters

See accompanying process map 'process for which letter to send re possible s170'.

This process is to help you decide which closure letter to send to the controller. It does not replace the s170 process and you should consult the Criminal Investigations Team (CRIT) in the usual way.

The starting point is to consider what the controller is looking for from the ICO. You'll send a different template closure letter depending on your answer to this question.

You need to make an assessment of whether it seems the controller wants the ICO to pursue the individual who has obtained/disclosed/retained the data or not. We shouldn't expect the controller to use the language found in the legislation, though they may do so.

The factors you'll consider when making the decision on the starting point include:

- Does much of the breach report form relate to the individual/their actions rather than measures the controller had in place and actions they're taking to put the matter right?
- Is the controller looking for help getting the data back/preventing use of the data?
- Has the controller used the complaints form or made reference to wanting to complain about the individuals responsible?
- Does the controller make reference to or focus on the impact of the incident on their business?
- Has the controller found out about the ICO as an organisation that may be able to help fix the problem, rather than being aware of the ICO and its own breach reporting responsibilities already?

Answering yes to above factors tends to suggest the controller may want the ICO to take action against the individual involved in the incident. The list is not exhaustive.

If the controller seems to want the ICO to pursue the individual but CRIT are not going to investigate, you'll send a letter that addresses both the controller's responsibility to keep data secure and the s170 aspect.

If the controller does not seem to want the ICO to pursue the individual and CRIT are not going to investigate, you'll treat the CRIT consultation and response as an internal process. You'll send a standard closure letter and only address the security aspects, as you would in a case that doesn't involve a possible s170 issue. You may still need to give advice about how

to prevent a similar incident in future, such as being clear to staff what information they can/can't access.

A controller may challenge your decision or want more information. It's possible you will decide they didn't want the ICO to pursue the individual, when they did.

We have created new letters for you to send in these situations, to allow you to explain your decision in more detail. If the controller is dissatisfied following a second letter, a manager will carry out a case review.

Laura Middleton
1 December 2021

Does it appear the DC has reported the incident to the ICO so we can pursue the individual? [See factors to help make this decision]

Yes/maybe

Consult CRIT at an appropriate point in the process [see s170 process map]

CRIT taking case?

Yes

Close case

No

Closure letter to address security breach aspect and our consideration of s170 offence(s) (Letter A)

Further response from DC, challenging decision? Consider second CRIT consult

New standard letter to provide more information about why a prosecution might not be taken forward, to be used in the event of challenge/as a final attempt to explain/resolve before a possible complaint (Letter D)

No

Consult CRIT at an appropriate point in the process [see s170 process map]

CRIT taking case?

Yes

Close case

No

Have CRIT asked DC to send investigation report when completed?

Yes

Closure letter to address security breach aspect, explain possible s170 offence(s) and invite DC to send additional information when they have completed their investigation, if they like (to include pointers of what to include in investigation) (Letter B)

More info received?

Closure letter needed if CRIT don't take the case after the additional information has been reviewed (Letter C)

Challenge?

New standard letter to provide more information about why a prosecution might not be taken forward, to be used in the event of challenge/as a final attempt to explain/resolve before a possible complaint (Letter D)

No

Close with standard PDB letter, or template if appropriate. Focus on security issue and do not mention consideration of s170 offence(s)

Request to consider s170? Consider second CRIT consult

Explain our view on s170 aspect (Letter E)

Date

Reference

Dear,

Personal data breach report of.

Thank you for reporting a personal data breach to the ICO. I am sorry to hear that a former employee has sent personal data to their private email address prior to leaving their employment for your organisation. .

To comply with data protection legislation, organisations need to have appropriate security measures in place to protect personal data. This includes measures to prevent employees sending personal data to personal email accounts.

The Data Protection Act 2018 creates an offence for a person to obtain, disclose or retain personal data without the consent of the data controller. The ICO can carry out criminal investigations and prosecute individuals where we believe an offence may have been committed.

We have considered whether it would be appropriate to conduct a criminal investigation concerning the sending of personal information to a personal email account. However, upon review of the information provided, we will not pursue an investigation due to the following reasons:

-

For these reasons, we are satisfied [name of DC] is taking the matter seriously and trying to put it right. The ICO does not need to take further action, though we will review this decision if we receive new information.

We recommend that you consider:
- Advice not related to preventing a recurrence

An important part of responding to a personal data breach is to take steps to prevent a recurrence. Advice about preventing a recurrence including contracts to set out how data is to be used, if relevant.

You may wish to consider taking legal advice about whether there are other steps you can take to pursue this matter.

If you'd like to learn more about your reporting obligations and wider data

protection responsibilities, there's lots of information on our website to help. You might like to start with our advice for small organisations: SME web hub – advice for all small organisations | ICO

I understand the decision not to pursue this matter further may be disappointing, but I hope you understand the reasons for our view.

Yours sincerely

Name
Title
Direct dial

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

Date

Reference:

Dear

Personal data breach report of date

Thank you for reporting a personal data breach to the ICO. I am sorry to hear that [description of incident that's causing difficulties] [and that this is causing difficulties for your business] if relevant. I apologise for the delay in writing to you.

To comply with data protection legislation, organisations need to have appropriate security measures in place to protect personal data. This includes measures to prevent the unauthorised access to and use of personal data check this is relevant to the incident described.

We have considered whether we need to take further action regarding [name of DC]'s compliance with data protection legislation, including the following factors:

- Reasons for closure

We have also considered whether [name of DC] had appropriate measures in place to protect the personal data.

- Reasons [if relevant and distinct from above]

For these reasons, we are satisfied [name of DC] is taking the matter seriously and trying to put it right. The ICO does not need to take further action, though we will review this decision if we receive new information.

We recommend that you consider:
Advice not related to preventing a recurrence

An important part of responding to a personal data breach is to take steps to prevent a recurrence. Advice about preventing a recurrence including We recommend providing clear advice to staff about what they can do, and shouldn't do, with personal data they have access to as part of their employment if relevant.

Thank you for reporting the incident. Further information and guidance relating to data security is available on our website.

Potential criminal offence

The Data Protection Act 2018 creates an offence for a person to obtain, disclose or retain personal data without the consent of the data controller. The ICO can carry out criminal investigations and prosecute individuals where we believe an offence may have been committed.

We have considered whether it would be appropriate to conduct a criminal investigation into [description of the incident], but we do not have sufficient information to decide. If you would like to send us a copy of your report once you have completed your investigation, we will be happy to reconsider.

We recommend your report includes information about:
- measures you had in place to prevent the incident
- how these measures were overcome
- whether the person had lawful access to this data as part of their role
- any action you have taken against the individual eg legal action, disciplinary action, etc
- any detriment suffered, or likely to be suffered by the data subjects
- Any other details from CRIT about what they'd like to be included

Yours sincerely

Name
Title
Direct dial

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

Date

Reference:

Dear

Additional information about personal data breach report

Thank you for providing additional information about a personal data breach [name of DC] experienced.

As we previously explained, the Data Protection Act 2018 creates an offence for a person to obtain, disclose or retain personal data without the consent of the data controller. The ICO can carry out criminal investigations and prosecute individuals where we believe an offence may have been committed.

We have considered whether it would be appropriate to conduct a criminal investigation into [description of the incident]. Information from CRIT to explain why we're not pursuing an investigation.

You may wish to consider taking legal advice about whether there are other steps you can take to pursue this matter.

I understand the decision not to pursue this matter further may be disappointing, but I hope you understand the reasons for our view.

Yours sincerely

Name
Title
Direct dial

Date

Reference:

Dear

Thank you for your email of [date]. I understand you are disappointed because we do not intend to take action against the individual(s) that [description of the incident]. I would like to provide some additional information to explain our decision.

Any new information from CRIT.

Useful paragraphs from below and any additional relevant information to be inserted here

The Information Commissioner is a publicly funded body and therefore must we target resources in a manner that will best serve the public interest.

Having considered this case carefully, in line with our regulatory action policy, we have decided not to take any further action in respect of [the individual responsible for the breach/name].

I understand this may be disappointing but I hope you understand the reasons for our decision.

Yours sincerely

Name
Title
Direct dial

Useful paragraphs to include, depending on the circumstances of the case:

The main purpose of the legislation is to protect the rights of individuals, not to protect business or commercial interests.

In making this assessment we have considered the level of detriment likely to be caused to the individuals affected. In this case it is considered unlikely such detriment will arise due to the nature and potential use of the information taken.

Date

Reference:

Dear

Personal data breach report of [date]

Thank you for your email of [date]. I understand you would like the ICO to consider taking action against the individual(s) that [description of incident].

The Data Protection Act 2018 creates an offence for a person to obtain, disclose or retain personal data without the consent of the data controller. The ICO can carry out criminal investigations and prosecute individuals where we believe an offence may have been committed.

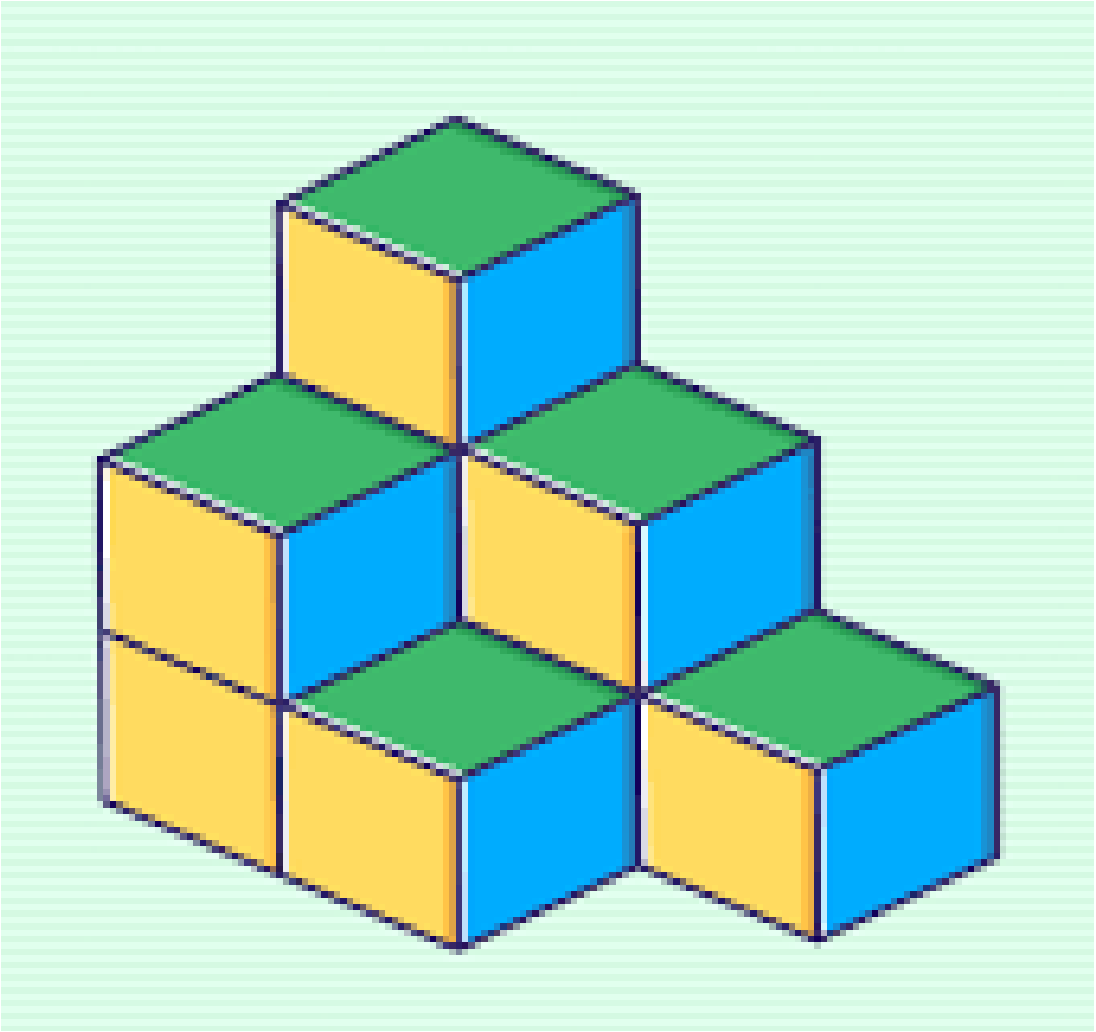
We have considered whether it would be appropriate to conduct a criminal investigation into [description of the incident]. Information from CRIT to explain why we're not pursuing an investigation.

You may wish to consider taking legal advice about whether there are other steps you can take to pursue this matter.

I understand the decision not to pursue this matter further may be disappointing, but I hope you understand the reasons for our view.

Yours sincerely

Name
Title
Direct dial



How many cubes are there?

Criminal Offences Under DPA 18

Section 170

Unlawful obtaining etc of personal data

(1) It is an offence for a person knowingly or recklessly:

(a) to obtain or disclose personal data without the consent of the controller,

(b) to procure the disclosure of personal data to another person without the consent of the controller, or

(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

Section 171

Re-identification of de-identified personal data

(1) It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

Section 173

Alteration etc of personal data to prevent disclosure to data subject

(1)Subsection (3) applies where—

(a) a request has been made in exercise of a data subject access right, and

(b) the person making the request would have been entitled to receive information in response to that request.

(3) It is an offence for a person listed in subsection (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

(4) Those persons are —

a) the controller, and

b) a person who is employed by the controller, an officer of the controller or subject to the direction of the controller.

Example 1

A response to a subject access request was sent to the mother of a child by email. This contained information relating to a child protection assessment. This assessment contained names of social workers and information about the individual who made the initial referral to social services. The person making the referral was a relative and wanted to remain anonymous due to ongoing issues with the family. The council sending these documents had taken time to redact the information to ensure that the any information identifying the referrer was kept confidential. The mother receiving the information has a friend who works with computers and has provided the information to them to reveal the identity of the referrer. Their friend was able to remove the redaction on the document and the mother has contacted the relative and threatened them.

Which potential offence is present here?

Example 2

An employee had been working for an insurance company. They have left the organisation and are going to work for a competitor. Within their role they dealt with new customers to bring in sales for the company. They would handle customer information such as name, contact details and some information about their insurance package. The company have been contacted by some of their customers asking why they insurance was being transferred to another organisation. The company investigated and found that the employee had emailed customer information to a personal account before they had left the organisation.

What potential offence is present here?

Example 3

A school have received a subject access request from a previous employee. They have requested information relating to an investigation which resulted in a dismissal. Within some of this information there were some manager comments which were of a discriminatory nature about the employee. When reviewing the information to send out to the individual the school did not want to share the manager's comments with the individual as they believed this would help their tribunal case. The school proceeded to destroy the documents which contained the managers comments so they could not be provided to the data subject.

Which potential offence is present here?

Regulatory Action Policy

- To respond swiftly and effectively to breaches of legislation which fall within the ICOs remit;
- To take action proportionately and exercise discretion as to when, in what manner, and to what extent enforcement is required, and;
- We will be selective when exercising this discretion, looking at the features and context of each case, as well as applying our resources more broadly to areas of greatest risk and potential or actual harm to the community.

For CRIT to take action

1. Has a criminal offence been committed?
2. Is there evidence
3. If there is no evidence can this be provided following further investigation?
4. Is it in the public interest?
5. Has there been any admission of responsibility?
6. Has the incident been reported to any other authorities?
7. Did the individual have legitimate access?

Assessing these cases

- Nature of the personal data?
- How was it obtained?
- What is the motive of the individual?
- What policies and procedures were in place?
- Did they have technical security measures?
- Did they have agreements in place?
- Did the individual responsible have legitimate access to the data?
- Any evidence of detriment?
- Has the controller taken steps to contain?
- Has the controller taken steps to limit the impact?
- Has any other action been taken by the controller?
- Have they identified any further measures?

When to RFI a S170-173 case?

- Do we need any more information to assess the controller's compliance?
- Do we have enough information to make an assessment on the breach element of the case?
- Do we need more information to decide whether to refer the case to civil?

- NOTE: If crit have requested further information to pursue the criminal aspect, we do not need to necessarily request this from the controller. You will need to make your own assessment on whether further information is needed.

Case examples

Advice to provide to data controllers

- Breach containment
- Notifying data subjects
- Mitigating any risk to the data subjects
- Review processes
- Review employee and third-party contracts
- Review staff training
- Review technical measures
- Legal action they could take
- Notifying other authorities
- Managing expectations

Vishing

- Voice phishing
- Vishing attacks usually come from an individual being tricked over the phone to grant access to particular types of personal data.
- Refer to CRIT in the usual way.
- Cyber incidents following the attack should be referred to the Cyber Incidents Team.

Any questions?

SLIDE 1

Visual puzzle – answer 9

SLIDE 2

Introduction

This sessions we will be going through the potential criminal offences under the DPA.

- We will be explaining what the criminal offences under the data protection act are
- Our Regulatory Action Policy
- Considerations when picking up these cases
- How we deal with these cases
- How we respond to these cases

Under the DPA 2018 there are three potential criminal offences and the ICO have the power to conduct a criminal investigation and prosecute individuals where we believe one of these has been committed. This session we will go through these potential offences and what to do when you are dealing with any related cases.

SLIDE 3

SECTION 170

S170 relates to the unlawful obtaining of personal data. The legislation states:

1. It is an offence for a person knowingly or recklessly -

a) to obtain or disclose personal data without the consent of the controller

b) to procure the disclosure of personal data to another person without the consent of the controller, or

c) after obtaining personal data to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

S170 subsection (3) also makes it an offence to retain personal data without the consent of the data controller.

This is the most common on that you will deal with on PDB. If an organisation experiences a personal data breach which is also potentially a section 170 offence, the data controller will need to report it to the PDB team in the usual way (phone or web form). We will consider the report under a two-tier process:

1. If we identify a Section 170 offence, we will refer the case on to the Criminal Investigation Team (CRIT) in the first instance and they will identify whether there is enough evidence to substantiate a criminal offence. This will be assessed in line with the ICOs regulatory action policy.
2. If CRIT can't take the case forward, it'll come back to the PDB team, and we will assess it in the normal way (i.e. whether they have appropriate technical and organisational measures in place to protect the personal data they control and process).

Under the DPA section 170 now creates an offence for an individual to retain information without the consent of the controller. Any cases where an individual is retaining information should be referred to CRIT for consideration. This could relate to an employee keeping hold of data, or a recipient refusing to delete information received in error.

If an individual has obtained personal data as a result of a personal data breach and wishes to retain it as proof of the breach or evidence in other proceedings, they should be advised that this data must be returned or disposed of. The recipient of the data can request written confirmation from the data controller that material was disclosed in error, but the personal data itself should be destroyed or returned as directed by the DC. Under no circumstances should the recipient be advised to retain the data.

SLIDE 4

Section 171

The next two potential offences are less common. The section 171 relates to the re-identification of data

1. It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

So this could relates to an individual intentionally un-redacting informaiton that has been redacted by the controller before sending to find out the identity of individuals.

SLIDE 5

Section 173 relates to the alteration of personal data to prevent disclosure.

1. Subsection (3) applies where –

a) A request has been made in exercise of a data subject's access rights, and

b) The person making the request would have been entitled to receive information in response to that request.

2. It is an offence for a person listed in subsection (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

As I say these cases are less common and could be likely you don't come across one of these cases. If you do it would be referred to CRIT as you would with the S170 offence.

SLIDE 6

Example 1 – answer S171

SLIDE 7

Example 2 – answer S170

SLIDE 8

Example 3 – answer S173

SLIDE 9

In addition to considering the criminal offence itself, we also need to consider the ICO's Regulatory Action Policy.

The ICO has enforcement powers, and we must use them predictably, consistently and judiciously.

- We must respond swiftly and effectively to breaches of legislation which fall within the ICO's remit, focussing on
  - those involving highly sensitive information,
  - those adversely affecting large groups of individuals,
  - those impacting vulnerable individuals.

- We will take proportionate action, we will exercise discretion as to when, in what manner, and to what extent enforcement is required;

- We will be selective when exercising this discretion, looking at the features and context of each case, as well as applying our resources more broadly to the areas of greatest risk and potential or actual harm to the community.

As a general principle, the more serious, high-impact, intentional, wilful, neglectful or repeated breaches can expect stronger regulatory action.

SLIDE 10

Considerations for CRIT to take action:

1. Firstly, they would then be considering the potential offence and the actions of the alleged perpetrator. Crit will be looking at whether an offence has a criminal offence been committed, does it fall under sections 170-173?
2. Then they would be looking at whether there is sufficient evidence to support a prosecution in this case? Criminal cases have to prove beyond all reasonable doubt that a criminal offence has taken place. (This is a higher threshold than a civil case where cases are proved on the 'balance of probabilities').
3. If they don't have the evidence at the time, then CRIT might consider whether it is likely they can provide this further down the line.
4. Is it in the public interest to prosecute this case? They would be looking at here the level of detriment the incident could cause to the individuals affected, the volume of information and how many people have been affected. Essentially, the higher the risk to members of the public the more likely it is they will take action.
5. Has there been an admission of responsibility? So have they been able to identify the person responsible. If a controller is unable to identify the individual there, we would be unable to take action.
6. Have any other authorities been informed? If any other authorities have been told about the incident this would be taken into consideration. If the police have been informed and are conducting their own investigation CRIT will not conduct a dual investigation. Generally, this is because the police have higher powers to prosecute individuals, and this would normally be for a more serious offence then an offence under the DPA.
7. Did the individual have legitimate access to the data at the time of the incident. When looking at this they would be considering whether the information has been lawfully obtained or unlawfully obtained. If the individual didn't have legitimate access this would be considered unlawful obtaining. If they did have legitimate access then CRIT would be looking at evidence provided by the controller that they have clear policies that set out their requirements when handling information. e.g employment contracts.

SLIDE 11

So, if CRIT don't take the case after their review this will come back to us to consider. Although we may provide advice on the reasons, we are not taking criminal action we will be overall making the assessment of the personal data breach aspect. We will be assessing the controllers compliance with the legislation and their actions in response to the breach. Often controllers can forget this aspect of self-reporting but we will be considering whether any further action is required against the organisation too. This assessment will be made in a similar way to any other case you pick up.

Some things we will be looking at:

- **The nature of the personal data** – so like we would a normal breach we would be looking at the level of sensitivity of the informaiton that has been impacted.
- **How this was obtained** – this could help give some context of the controllers measures. For example, if it was accessed or obtained inappropriately by a person who did not have legitimate access to the data we would be looking at whether they had anything in place to protect it.
- **What was the motivation of the individual** – this again would give you some context on the situation.
    - Did the individual have malicious intent?
    - Was the access intentional or unintentional?
    - What do they plan on doing with the information.

  We often get report of individuals emailing data to their personal accounts. Understanding why they have done this can help to determine the level of risk. So if they had done this without knowing the rules would have a different risk level to an individual emailing data knowingly to then use it further.

- **What policies and procedures are in place?** – so this would be where we are considering whether a controller had the appropriate measures in place to stop this from happening. Has the organisation made sure staff are aware of what they can and can't do with information.
- **Technical security** – were there access controls in place, password protection on documents, were the correct permissions set. Did the controller have sufficient controls in place to protect against the unauthorised access or obtaining of information?
- **What agreements are in place with staff members** – so did the controller have appropriate agreements in place and were these made clear to staff members. If a controller had clearly outlined to staff what they should be doing with information we are less likely to be taking action against an organisation.

- **Did they have legitimate access to the data** – this could also be a factor that we consider on PDB. For example, if there were agreements in place and the individual had legitimate access this could suggest that the individual was acting outside of the controls that were in place which might be considered a reason for closure.
- **Is there any evidence of detriment to the individuals** – as usual we will be looking at the level of detriment caused to the individuals affected. It is important to remember we are looking at the individual when considering this and not the detriment potentially caused to a business.
- **Have steps been taken to contain** – like we would with any breach we would be looking at whether the controller has taken steps to contain the incident and regain control of the data? So, have they issued written communications to individual to request that they cease using information or delete data. Have they revoked access to systems or email accounts?
- **Have steps been taken to limit the impact** – so what has been done here by the controller to reduce the risk to the data subject. For example, relocating an individual where address information has been accessed which could put them at risk. Or contacting individuals to advise them of potential unwanted contact. Has the controller acted appropriately in response to this or have they neglected to take action to help limit any impact?
- **What action has been taken by the controller** – this could cover a range of actions depending on the incident itself. They could be taking steps to review the permissions on systems and revoke access. This could be in relation to disciplinary action or any internal investigations they are conducting. Overall, here we will be looking whether they are taking steps to address what has happened.
- **Have any further measures been identified** – we would need to look at what the controller is doing to prevent another incident occurring. They could be reviewing contracts, implementing further training or tightening up their technical security. They should be looking at lessons they could learn from the incident to strengthen what is already in place.

SLIDE 12

When to RFI a S170 to 173 case?

You will need to review the case and consider:

- **Do we need any more information to assess the controllers compliance?** – this would be from a breach perspective. Do we have enough information in the report to assess their compliance or

do we need to get some more informaiton about their technical and organisational measures.

- **Do we have enough information to make an assessment on the breach element of the case?** – do we know enough about how this happened the circumstances surrounding this, the risk to the DS and how the controller is responding. Or do we need more information to make this assessment?
- **Do we need more information to decide whether to refer the case to civil?** Is there a chance that we might need to refer the case to civil for further action, but need more information to decide then we would go out for more information on these cases.

  Occasionally you may get a response on a case to refer to civil for consideration. This shouldn't be done as standard you will need to make you own assessment on whether this needs to be referred.

You might pick up reports when working through the queue where CRIT have asked for more information to pursue the criminal aspect of the case. We do not need to necessarily request this from the controller. It's important to remember that we don't need to go out for the extra information needed by CRIT alone you will need to make your own assessment on whether we need more information on the personal data breach aspect.

SLIDE 13

Case examples:

[redacted]

[redacted]

[redacted]

SLIDE 15

Ask trainees what kinds of things they can think of the recommend in these cases?

Some most common recommendations you may provide to data controllers in respect to s170 cases are:

- **Containing the breach:** DCs should take steps to recover the data, or contain the breach as far as is practicable. They may request written confirmation from the recipient who received the information in error that they have deleted it or not shared it further.

- **Notifying data subjects:** DCs should consider the likely risk to the affected individuals, as if it is likely there is a high risk then they will need to inform the affected individuals. They should consider whether informing the affected individuals will allow them to take steps to protect themselves from any potential harm.
- **Mitigating any risk to the data subjects:** The DC should consider if there are any steps they could take to help mitigate any potential risk or detriment to the affected data subjects. For example, if individuals are at an increased risk of identity theft, the DC can provide them with credit monitoring service or appropriate advice.
- **Review processes:** The DC should conduct a root cause analysis and review their processes to determine if there are any additional measures they could implement to prevent a reoccurrence.
- **Review employee and third party contracts:** DCs may wish to review the contracts in place with staff and third parties to ensure this makes clear staff requirements when handling personal data on behalf of the organisation. This should clarify who controls information and what happens to the personal data when an employee leaves or a contract ends.
- **Review staff training:** DCs should provide adequate, role based training to staff. This training should make clear to staff how to appropriately handle personal data on behalf of the organisation. In particular, this should make clear that information should not be accessed or shared without a business need to do so or authorisation from the organisation.
- **Review technical measures:** The organisation should review any technical controls they have in place or could implement to keep personal data secure and to ensure that data is only available to staff who need access to this in line with their job role. They could also conduct periodic audits to monitor staff adherence.
- **Legal action they could take:** The DC may wish to consider pursuing the incident via a legal route, for example, issuing a cease and desist letter to the responsible individual. They may also be able to pursue a breach of employment contract depending on what measures they had in place prior to the incident.
- **Notifying other authorities:** DCs should consider whether they need to notify the Police as they oversee the Theft Act and the Computer Misuse Act. They should also consider whether they’re duty bound to report incidents of this nature to any other regulatory authorities, or licencing authorities.
- **Managing expectation -**

In certain circumstances we may need to manage the expectation of DCs who have reported potential s170 incidents to us. In particular, this tends to centre around the action that we will take in response to these incidents. For example, a former employee who has taken client data as they are setting up their own business or they are now working for a rival company.

You may need to explain that the main purpose of the DPA 2018 is to protect the rights of individuals in respect of personal information which relates to them, not to protect the commercial interests of organisations who hold that information. It is not the ICO's policy to pursue 'business to business' matters where little or no detriment has been caused to data subjects. In most cases, unwanted contact for marketing purposes is unlikely to cause significant detriment beyond annoyance.

It may be helpful to explain that the ICO is publicly funded and has limited resources and therefore needs to be selective with regard to the cases it can prosecute. Decisions are made in accordance with the ICO's Regulatory Action Policy.

Cases brought under s.170 – 173 of the DPA 2018 are heard in the Criminal Court and have to be proven to the criminal standard, i.e. beyond all reasonable doubt. Individuals may seek to bring private prosecutions, but these would have to be proven to the same standard and the authority of the ICO or the DPP would be required before the matter could be brought before the courts.

As mentioned above, an individual can commence a civil action, which would be to the civil burden of proof i.e. on the balance of probabilities, a lower burden than the criminal burden. Anyone seeking to do this should be advised to obtain independent legal advice.

SLIDE 15

Another type of incident which we refer to our Criminal Investigations team is known as a vishing attack.

The term 'vishing' comes from a combination of the words 'voice' and 'phishing'. As this combination indicates, vishing attacks usually come from an individual being tricked over the phone to grant access to particular types of personal data.

A common example of a vishing attack would be an individual receiving a call from someone purporting to be their IT provider and requesting remote access to their computer to fix a problem. After gaining access, they will then often delete files from the computer and demand money from the individual. Another common target for vishing attacks are hotels and restaurants, who will receive calls from someone purporting to be

their reservation or booking system provider. Once they gain access to the system, they will use the customer details to contact them directly and request money to secure the booking.

If the case relates to a Vishing attack, then the case is dealt with in the same way as a section 170 case, with a consult sent to CRIT before assessing the case for closure or referral in the usual way. This is because the root cause of the data compromise is not a cyber incident. If the Vishing attack led to a cyber incident however, such as malware or ransomware, you would refer this to our Cyber Investigations team.

If you pick up a Vishing case, you can flag this with us and release it to the main PDB queue to be dealt with by a PDB member of staff.

Case example

[redacted] – Vishing.

SLIDE 16

Any questions?

Section 170-173 Overview

PDB Service

S170 DPA 2018

Unlawful obtaining etc of personal data

(1) It is an offence for a person knowingly or recklessly —

(a) to obtain or disclose personal data without the consent of the controller,

(b) to procure the disclosure of personal data to another person without the consent of the controller, or

(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

S171 DPA 2018

Re-identification of de-identified personal data

(1) It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

S173 DPA 2018

Alteration etc of personal data to prevent disclosure to data subject

(1)Subsection (3) applies where—

(a) a request has been made in exercise of a data subject access right, and

(b) the person making the request would have been entitled to receive information in response to that request.

(3) It is an offence for a person listed in subsection (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

(4) Those persons are —

(a) the controller, and

(b) a person who is employed by the controller, an officer of the controller or subject to the direction of the controller.

For CRIT to take action

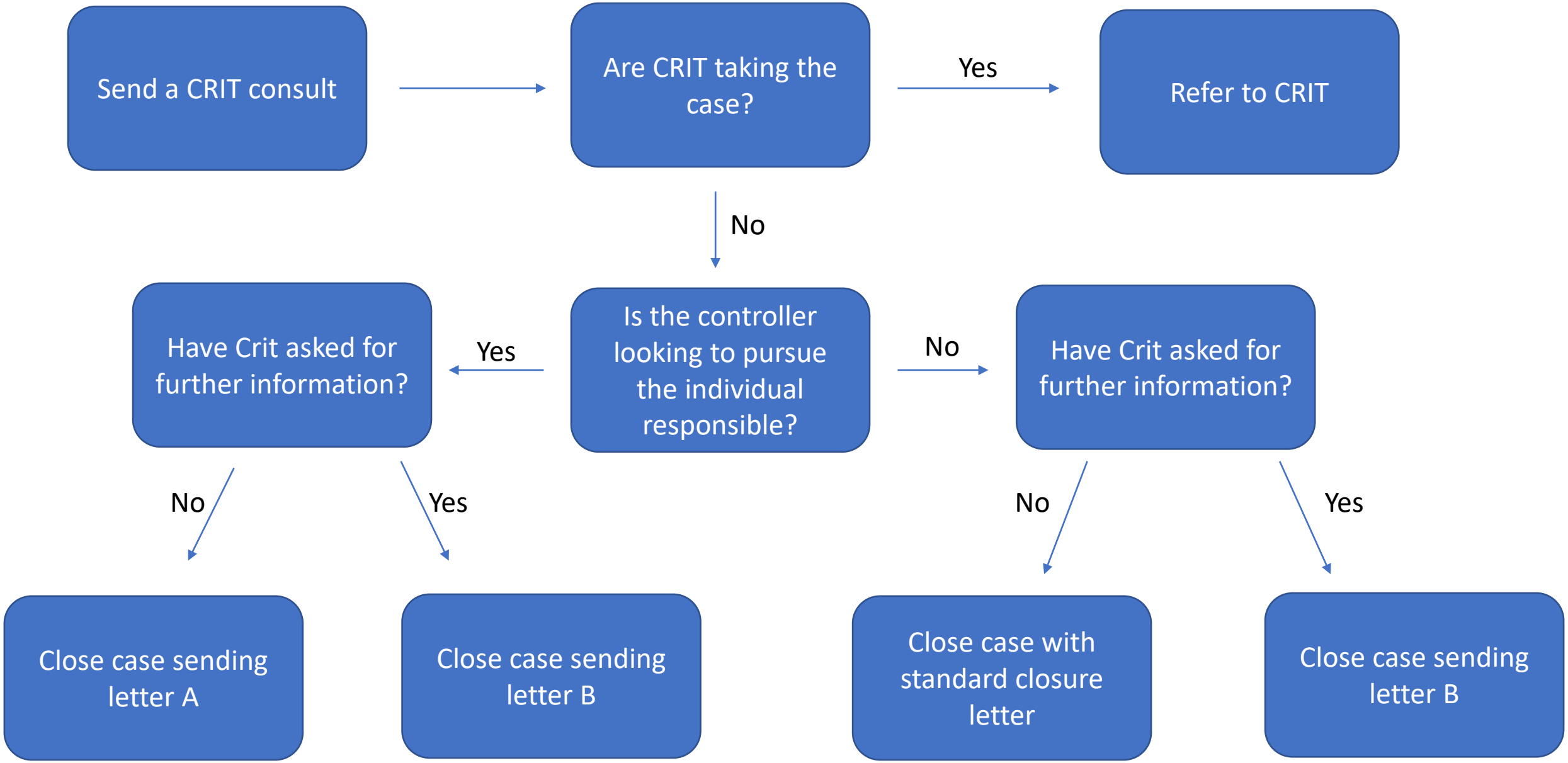
Assessing S170-173 cases

- ❑ Nature of the personal data
- ❑ How was it obtained?
- ❑ What is the motive of the individual?
- ❑ What policies and procedures were in place?
- ❑ Did they have technical security measures?
- ❑ Did they have agreements in place?
- ❑ Did the individual responsible have legitimate access to the data?
- ❑ Any evidence of detriment?
- ❑ Has the controller taken steps to contain?
- ❑ Has the controller taken steps to limit the impact?
- ❑ Has any other action been taken by the controller?
- ❑ Have they identified any further measures?

When to RFI a S170-173 case?

- Do we need any more information to assess the controllers compliance?
- Do we have enough information to make an assessment on the breach element of the case?
- Do we need more information to decide whether to refer the case to civil?

NOTE: If crit have requested further information to pursue the criminal aspect we do not need to necessarily request this from the controller. You will need to make your own assessment on whether further information is needed.


Send a CRIT consult
Are CRIT taking the case?
Yes
Refer to CRIT
No
Is the controller looking to pursue the individual responsible?
Yes
Have Crit asked for further information?
No
Close case sending letter A
Yes
Close case sending letter B
No
Have Crit asked for further information?
No
Close case with standard closure letter
Yes
Close case sending letter B

Advice to provide to data controllers

- ❑ Breach containment
- ❑ Notifying data subjects
- ❑ Mitigating any risk to the data subjects
- ❑ Review processes
- ❑ Review employee and third party contracts
- ❑ Review staff training
- ❑ Review technical measures
- ❑ Legal action they could take
- ❑ Notifying other authorities

Other cases we refer to CRIT

Vishing

- ❑ Text message
- ❑ Social Media
- ❑ Phone

Case examples

SLIDE 1

Introduction

This sessions we will be going through the potential criminal offences under the DPA.

- We will be explaining what the criminal offences under the data protection act are
- Our Regulatory Action Policy
- Considerations when picking up these cases
- How we deal with these cases
- How we respond to these cases

Under the DPA 2018 there are three potential criminal offences and the ICO have the power to conduct a criminal investigation and prosecute individuals where we believe one of these has been committed. This session we will go through these potential offences and what to do when you are dealing with any related cases.

SLIDE 2

SECTION 170

S170 relates to the unlawful obtaining of personal data. The legislation states:

1. It is an offence for a person knowingly or recklessly -

a) to obtain or disclose personal data without the consent of the controller

b) to procure the disclosure of personal data to another person without the consent of the controller, or

c) after obtaining personal data to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

S170 subsection (3) also makes it an offence to retain personal data without the consent of the data controller.

This is the most common on that you will deal with on PDB. If an organisation experiences a personal data breach which is also potentially a section 170 offence, the data controller will need to report it to the PDB team in the usual way (phone or web form). We will consider the report under a two-tier process:

1. If we identify a Section 170 offence, we will refer the case on to the Criminal Investigation Team (CRIT) in the first instance and they will identify whether there is enough evidence to substantiate a

criminal offence. This will be assessed in line with the ICOs regulatory action policy.

2. If CRIT can't take the case forward, it'll come back to the PDB team, and we will assess it in the normal way (i.e. whether they have appropriate technical and organisational measures in place to protect the personal data they control and process).

Under the DPA section 170 now creates an offence for an individual to retain information without the consent of the controller. Any cases where an individual is retaining information should be referred to CRIT for consideration. This could relate to an employee keeping hold of data, or a recipient refusing to delete information received in error.

If an individual has obtained personal data as a result of a personal data breach and wishes to retain it as proof of the breach or evidence in other proceedings, they should be advised that this data must be returned or disposed of. The recipient of the data can request written confirmation from the data controller that material was disclosed in error, but the personal data itself should be destroyed or returned as directed by the DC. Under no circumstances should the recipient be advised to retain the data.

SLIDE 3

Section 171

The next two potential offences are less common. The section 171 relates to the re-identification of data

1. It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

So this could relates to an individual intentionally un-redacting informaiton that has been redacted by the controller before sending to find out the identity of individuals.

SLIDE 4

Section 173 relates to the alteration of personal data to prevent disclosure.

1. Subsection (3) applies where –

    a) A request has been made in exercise of a data subject's access rights, and

b) The person making the request would have been entitled to receive information in response to that request.

2. It is an offence for a person listed in subsection (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

As I say these cases are less common and could be likely you don't come across one of these cases. If you do it would be referred to CRIT as you would with the S170 offence.

SLIDE 5

Considerations for CRIT to take action:

1. Firstly, they would then be considering the potential offence and the actions of the alleged perpetrator. Crit will be looking at whether an offence has a criminal offence been committed, does it fall under sections 170-173?
2. Then they would be looking at whether there is sufficient evidence to support a prosecution in this case? Criminal cases have to prove beyond all reasonable doubt that a criminal offence has taken place. (This is a higher threshold than a civil case where cases are proved on the 'balance of probabilities').
3. If they don't have the evidence at the time, then CRIT might consider whether it is likely they can provide this further down the line.
4. Is it in the public interest to prosecute this case? They would be looking at here the level of detriment the incident could cause to the individuals affected, the volume of information and how many people have been affected. Essentially, the higher the risk to members of the public the more likely it is they will take action.
5. Has there been an admission of responsibility? So have they been able to identify the person responsible. If a controller is unable to identify the individual there, we would be unable to take action.
6. Have any other authorities been informed? If any other authorities have been told about the incident this would be taken into consideration. If the police have been informed and are conducting their own investigation CRIT will not conduct a dual investigation. Generally, this is because the police have higher powers to prosecute individuals, and this would normally be for a more serious offence then an offence under the DPA.
7. Did the individual have legitimate access to the data at the time of the incident. When looking at this they would be considering

whether the information has been lawfully obtained or unlawfully obtained. If the individual didn't have legitimate access this would be considered unlawful obtaining. If they did have legitimate access then CRIT would be looking at evidence provided by the controller that they have clear policies that set out their requirements when handling information. e.g employment contracts.

SLIDE 6

So, if CRIT don't take the case after their review this will be something that comes back to us to consider. Although we may provide advice on the reasons, we are not taking criminal action we will be overall making the assessment of the personal data breach aspect. We will be assessing the controllers compliance with the legislation and their actions in response to the breach. Often controllers can forget this aspect of self-reporting but we will be considering whether any further action is required against the organisation too.

Some things we will be looking at:

- **The nature of the personal data** – so like we would a normal breach we would be looking at the level of sensitivity of the informaiton that has been impacted.
- **How this was obtained** – this could help give some context of the controllers measures. For example, if it was accessed or obtained inappropriately by a person who did not have legitimate access to the data we would be looking at whether they had anything in place to protect it.
- **What was the motivation of the individual** – this again would give you some context on the situation. Did the individual have malicious intent? Was the access intentional or unintentional? What do they plan on doing with the information. We often get report of individuals emailing data to their personal accounts. Getting the context of the motive can help to determine the level of risk. So if they had done this without knowing the rules would have a different risk level to an individual emailing data to then use it further.
- **What policies and procedures are in place?** – so this would be where we are considering whether a controller had the appropriate measures in place to stop this from happening.
- **Technical security** – were there access controls in place, password protection on documents, were the correct permissions set. Did the controller have sufficient controls in place to protect against the unauthorised access or obtaining of information?

- **What agreements are in place with staff members** – so did the controller have appropriate agreements in place and were these made clear to staff members. If a controller had clearly outlined to staff what they should be doing with information we are less likely to be taking action against an organisation.
- **Did they have legitimate access to the data** – this could too be a factor we consider. If the agreements were there and the individual had legitimate access could suggest that the individual was acting outside of the controls that were in place which might be considered a reason for closure.
- **Is there any evidence of detriment to the individuals** – as normally we will be looking at the level of detriment caused to the individuals affected. It is important to remember we are looking at the individual when considering this and not the detriment potentially caused to a business.
- **Have steps been taken to contain** – like we would with any breach has the controller taken steps to contain? Have they issued any written notification to the individual for them to delete information or cease using the data.
- **Have steps been taken to limit the impact** – so what has been done here by the controller to reduce the risk to the data subject. Have they acted appropriate in response to this or have they neglected to take action.
- **What action has been taken by the controller** – this could cover a range of actions depending on the incident itself. They could be taking steps to review the permissions on systems and revoke access. This could be in relation to an employee in regard to disciplinary action or any internal investigations they are conducting. Overall, here we will be looking whether they are taking steps to address what has happened.
- **Have any further measures been identified** – we would need to look at what the controller is doing to prevent another incident occurring. They could be reviewing contracts, implementing further training or tightening up their technical security. They should be looking at lessons they could learn within the incident and whether or not

SLIDE 7

When to RFI a S170 to 173 case?

You will need to review the case and consider:

- Do we need any more information to assess the controllers compliance? – this would be solely based on the breach perspective. Do we have enough information in the report to assess their

compliance or do we need to get some more informaiton about their technical and organisational measures.

- Do we have enough information to make an assessment on the breach element of the case? – do we know enough about how this happened the circumstances surrounding this, the risk to the DS and how the controller is responding. Or do we need more information to make this assessment?
- Do we need more information to decide whether to refer the case to civil? Is there a chance that we might need to refer the case to civil for further action but need more information to decide? CRIT may respond to some cases advising to refer to civil for consideration. This shouldn't be done as standard you will need to make you own assessment on whether this needs to be referred.

You might pick up reports when working through the queue where CRIT have asked for more information to pursue the criminal aspect of the case. We do not need to necessarily request this from the controller. It's important to remember that we don't need to go out for the extra information needed by CRIT alone you will need to make your own assessment on whether we need more information from a personal data breach perspective.

SLIDE 8

- Talk through flow chart to help decide which letter to use

SLIDE 9

Some most common recommendations you may provide to data controllers in respect to s170 cases are:

- **Containing the breach:** DCs should take steps to recover the data, or contain the breach as far as is practicable. They may request written confirmation from the recipient who received the information in error that they have deleted it or not shared it further.
- **Notifying data subjects:** DCs should consider the likely risk to the affected individuals, as if it is likely there is a high risk then they will need to inform the affected individuals. They should consider whether informing the affected individuals will allow them to take steps to protect themselves from any potential harm.
- **Mitigating any risk to the data subjects:** The DC should consider if there are any steps they could take to help mitigate any

potential risk or detriment to the affected data subjects. For example, if individuals are at an increased risk of identity theft, the DC can provide them with credit monitoring service or appropriate advice.

- **Review processes:** The DC should conduct a root cause analysis and review their processes to determine if there are any additional measures they could implement to prevent a reoccurrence.
- **Review employee and third party contracts:** DCs may wish to review the contracts in place with staff and third parties to ensure this makes clear staff requirements when handling personal data on behalf of the organisation. This should clarify who controls information and what happens to the personal data when an employee leaves or a contract ends.
- **Review staff training:** DCs should provide adequate, role based training to staff. This training should make clear to staff how to appropriately handle personal data on behalf of the organisation. In particular, this should make clear that information should not be accessed or shared without a business need to do so or authorisation from the organisation.
- **Review technical measures:** The organisation should review any technical controls they have in place or could implement to keep personal data secure and to ensure that data is only available to staff who need access to this in line with their job role. They could also conduct periodic audits to monitor staff adherence.
- **Legal action they could take:** The DC may wish to consider pursuing the incident via a legal route, for example, issuing a cease and desist letter to the responsible individual. They may also be able to pursue a breach of employment contract depending on what measures they had in place prior to the incident.
- **Notifying other authorities:** DCs should consider whether they need to notify the Police as they oversee the Theft Act and the Computer Misuse Act. They should also consider whether they're duty bound to report incidents of this nature to any other regulatory authorities, or licencing authorities.

In certain circumstances we may need to manage the expectation of DCs who have reported potential s170 incidents to us. In particular, this tends to centre around the action that we will take in response to these incidents. For example, a former employee who has taken client data as they are setting up their own business or they are now working for a rival company.

You may need to explain that the main purpose of the DPA 2018 is to protect the rights of individuals in respect of personal information which relates to them, not to protect the commercial interests of organisations

who hold that information. It is not the ICO's policy to pursue 'business to business' matters where little or no detriment has been caused to data subjects. In most cases, unwanted contact for marketing purposes is unlikely to cause significant detriment beyond annoyance.

It may be helpful to explain that the ICO is publicly funded and has limited resources and therefore needs to be selective with regard to the cases it can prosecute. Decisions are made in accordance with the ICO's Regulatory Action Policy.

Cases brought under s.170 – 173 of the DPA 2018 are heard in the Criminal Court and have to be proven to the criminal standard, i.e. beyond all reasonable doubt. Individuals may seek to bring private prosecutions, but these would have to be proven to the same standard and the authority of the ICO or the DPP would be required before the matter could be brought before the courts.

As mentioned above, an individual can commence a civil action, which would be to the civil burden of proof i.e. on the balance of probabilities, a lower burden than the criminal burden. Anyone seeking to do this should be advised to obtain independent legal advice.

SLIDE 10

Another type of incident which we refer to our Criminal Investigations team is known as a vishing attack.

The term 'vishing' comes from a combination of the words 'voice' and 'phishing'. As this combination indicates, vishing attacks usually come from an individual being tricked over the phone to grant access to particular types of personal data.

A common example of a vishing attack would be an individual receiving a call from someone purporting to be their IT provider and requesting remote access to their computer to fix a problem. After gaining access, they will then often delete files from the computer and demand money from the individual. Another common target for vishing attacks are hotels and restaurants, who will receive calls from someone purporting to be their reservation or booking system provider. Once they gain access to the system, they will use the customer details to contact them directly and request money to secure the booking.

If the case relates to a Vishing attack, then the case is dealt with in the same way as a section 170 case, with a consult sent to CRIT before assessing the case for closure or referral in the usual way. This is because the root cause of the data compromise is not a cyber incident. If the Vishing attack led to a cyber incident however, such as malware or ransomware, you would refer this to our Cyber Investigations team.

If you pick up a Vishing case, you can flag this with us and release it to the main PDB queue to be dealt with by a PDB member of staff.

Any questions?

SLIDE 11

[redacted] - Letter B, a closure whilst inviting the DC to supply their investigation report.

[redacted] – Modified Letter A, a closure which covers S170 offence. (Report received via the reporting line which is best viewed via the rendition.

[redacted] – Standard closure letter.

[redacted] – Vishing.