Data Protection Act 1998

Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998

Data Protection Act 1998

Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998

Presented to Parliament pursuant to Section 55(C)(6) of the Data Protection Act 1998 as amended by Section 144 of the Criminal Justice and Immigration Act 2008

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at:

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

Print ISBN 9781474117111
Web ISBN 9781474117128

ID 24031511 03/15 48892 19585

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

Guidance about the issue of monetary penalties

Introduction

Under section 55A to 55E of the Data Protection Act 1998 (the "Act"), introduced by the Criminal Justice and Immigration Act 2008, the Information Commissioner (the "Commissioner") may, in certain circumstances, serve a monetary penalty notice on a data controller.

In addition, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (the "2011 Regulations") inserted section 55A to 55E of the Act into the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "2003 Regulations"), enabling the Commissioner to serve a monetary penalty notice on a person who breaches the 2003 Regulations.

A monetary penalty notice is a notice requiring a person to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice. The amount of the monetary penalty determined by the Commissioner must not exceed £500,000. The monetary penalty is not kept by the Commissioner, but must be paid into the Consolidated Fund owned by HM Treasury.

The Commissioner may impose a monetary penalty notice if a data controller has seriously contravened the Act or if any person has seriously contravened the 2003 Regulations and if, in both cases, the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the data controller or person must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.

The power to impose a monetary penalty notice is part of the Commissioner's overall regulatory regime which includes the power to serve an enforcement notice under section 40 of the Act, carry out a voluntary assessment under section 51(7) of the Act, serve an assessment notice under section 41A of the Act or carry out an audit under the 2003 Regulations as amended. It will be used as both a sanction and a deterrent against non-compliance with the statutory requirements.

The Commissioner may still serve an enforcement notice in relation to the same contravention if he is satisfied that positive steps need to be taken either by a data controller to achieve compliance with the data protection principle(s) in question or by a person to achieve compliance with the requirement(s) of the 2003 Regulations in question.

The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act or with the 2003 Regulations. The possibility of a monetary penalty notice should act as an encouragement towards compliance, or at least as a deterrent against non-compliance, on the part of all data controllers or persons.

It is clear from the wording of section 55A of the Act that a monetary penalty notice will only be appropriate in the most serious situations. Therefore in such cases the monetary penalty must be sufficiently meaningful to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening person and by others. This applies both in relation to the specific type of contravention and other contraventions more generally.

The Commissioner will take into account the sector, for example, whether the person is a voluntary organisation and also the size, financial and other resources of a person before determining the amount of a monetary penalty. The purpose of a monetary penalty notice is not to impose undue financial hardship on an otherwise responsible person.

At the same time the Commissioner considers that the proper handling of personal data in accordance with the Act and compliance with the requirements of the 2003 Regulations (where relevant) should not be seen as an extra requirement for businesses. Compliance with the Act and the 2003 Regulations (where relevant) is an integral part of the carrying out of any business activity.

Monetary penalty notices are only designed to deal with serious contraventions of the Act and the 2003 Regulations. At the same time there may be wide variations in the amount of the monetary penalty depending on the circumstances of each case. Minor contraventions may be subject to other enforcement procedures.

The Commissioner is committed to acting consistently, proportionately and in accordance with public law. Essentially, the Commissioner will use this power as a sanction against a person who deliberately or negligently disregards the law. However, it does not change his commitment to simplifying the Act and the 2003 Regulations where possible and making it easier for organisations to comply with their obligations under both the Act and the 2003 Regulations.

This is the statutory guidance issued under the Act. This means that the guidance has been approved by the Secretary of State and laid before Parliament. This guidance must, in particular, deal with the circumstances in which the Commissioner would consider it appropriate to issue a monetary penalty notice and how he will determine the amount of the monetary penalty.

This guidance is not concerned with the fixed £1,000 monetary penalty that the Commissioner can impose on service providers for a breach of the requirements to notify personal data breaches under Regulation 5A of the 2003 Regulations.

It should be read in conjunction with the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

This is the third edition of this guidance. The Commissioner will consider altering or replacing this guidance in the way provided for in the Act in the light of further experience of its application. Any such altered or replaced guidance will be published on the Commissioner's website after consultation with the Secretary of State.

For ease of reference this guidance is divided into the following sections:

Section 1	Brief overview
Section 2	Power to impose a monetary penalty
Section 3	Circumstances in which the Commissioner would consider it appropriate to issue a monetary penalty notice
Section 4	How the Commissioner will determine the amount of a monetary penalty together with the factors he will take into account when making such a decision
Section 5	Notice of Intent
Section 6	Provision for a data controller or person to make representations to the Commissioner before a final decision is made
Section 7	Monetary penalty notice
Section 8	Right of appeal against monetary penalty notice

1 Brief overview (see figure A below)

As a starting point the Commissioner will satisfy himself, by means of an investigation or otherwise, that he has the power to impose a monetary penalty in that there has been a serious contravention of the Act or the 2003 Regulations and that the other statutory requirements apply (see section 2 below).

He will then consider whether, in the circumstances, it would be appropriate to issue a monetary penalty notice (see section 3 below) and, if so, determine the amount of a monetary penalty (see section 4 below).

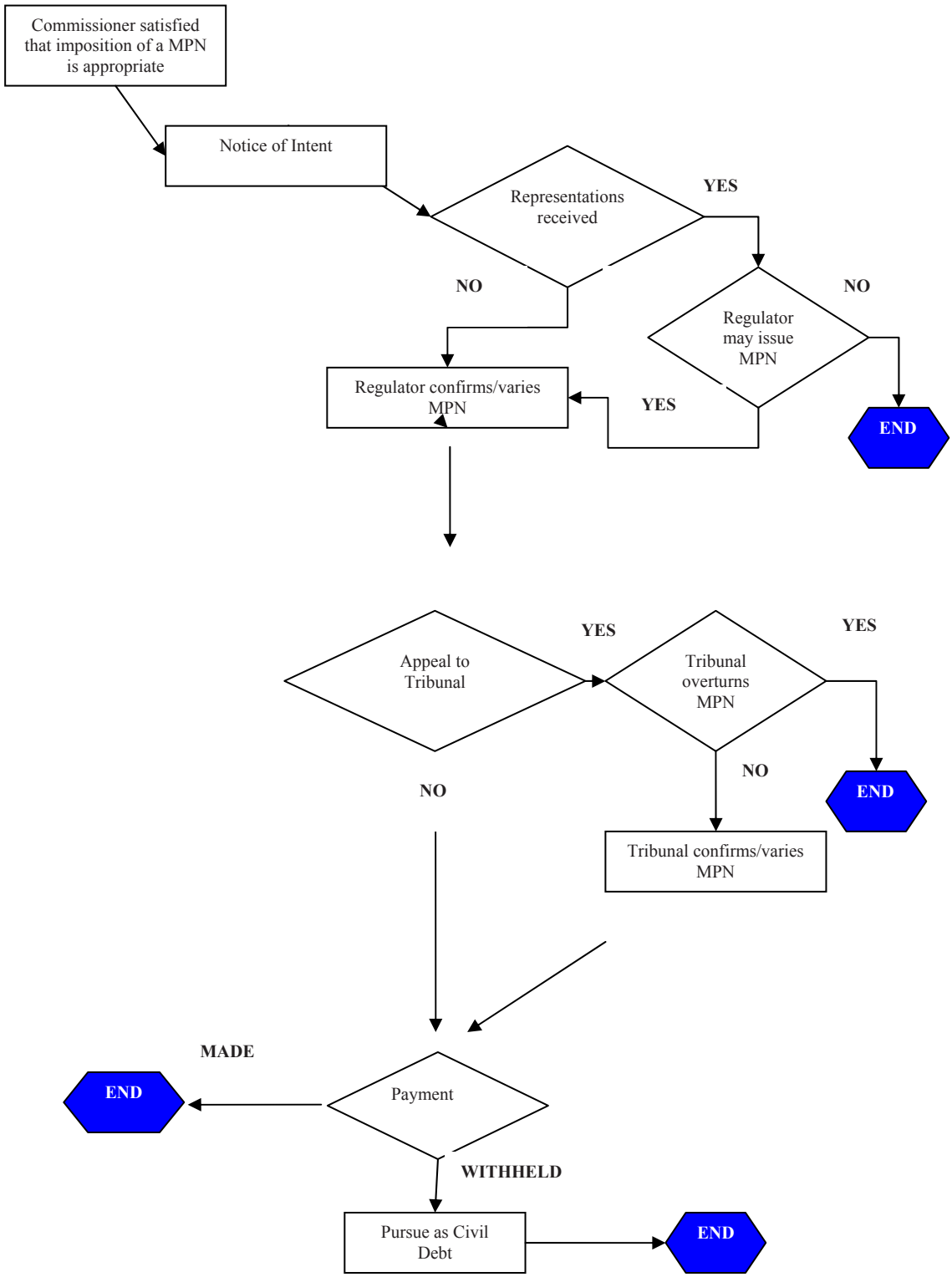
The Commissioner must initially serve a notice of intent if he proposes to serve a monetary penalty notice. The notice of intent will set out the proposed amount of the monetary penalty (see section 5 below).

The notice of intent will also inform the recipient that he may make written representations in relation to the Commissioner's proposal within a certain period of time (see section 6 below).

The Commissioner may then serve a monetary penalty notice requiring the person to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice (see section 7 below).

A person on whom a monetary penalty notice is served may appeal to the First-tier Tribunal (Information Rights) against the issue of the monetary penalty notice and/or the amount of the penalty specified in the notice (see section 8 below).

Figure A


Commissioner satisfied that imposition of a MPN is appropriate
Notice of Intent
Representations received
YES
NO
Regulator may issue MPN
NO
Regulator confirms/varies MPN
YES
END
Appeal to Tribunal
YES
Tribunal overturns MPN
YES
NO
END
NO
Tribunal confirms/varies MPN
MADE
END
Payment
WITHHELD
Pursue as Civil Debt
END

2 Power to impose a monetary penalty

The Act and the 2003 Regulations apply to the whole of the UK including Northern Ireland. Under the Act the power to impose a monetary penalty came into force on 6 April 2010 and under the 2003 Regulations on 26 May 2011. They do not apply retrospectively.

In relation to serious contraventions of the Act the power to impose monetary penalties applies to all data controllers in the private, public and voluntary sectors including, but not limited to; large companies, small businesses, sole traders, charitable bodies, voluntary organisations, Government Departments and office holders created by statute such as electoral registration officers.

A monetary penalty notice cannot be imposed on the Crown Estate Commissioners or a person who is a data controller by virtue of section 63(3) of the Act or a person who is not a data controller, for example, a bank employee or a Crown Servant such as a member of the Armed Forces or a volunteer for a charity. Nor can a monetary penalty be imposed on a data processor where processing of personal data is carried out on behalf of a data controller.

In relation to serious contraventions of the requirements of the 2003 Regulations a monetary penalty can be imposed on any person in the private, public and voluntary sectors. This can either be a legal person such as a business or a charity or a natural person, in other words a living individual but a penalty would not be imposed on an employee who was simply acting on the instructions of his employer.

The Commissioner will not impose a monetary penalty if to do so would result in the Commissioner acting inconsistently with any of his statutory duties. Nor will the Commissioner impose a monetary penalty for serious contraventions of the Act if the contravention was discovered in the process of the Commissioner carrying out a voluntary assessment on a data controller under section 51(7) of the Act or following compliance with an assessment notice served under section 41A of the Act.

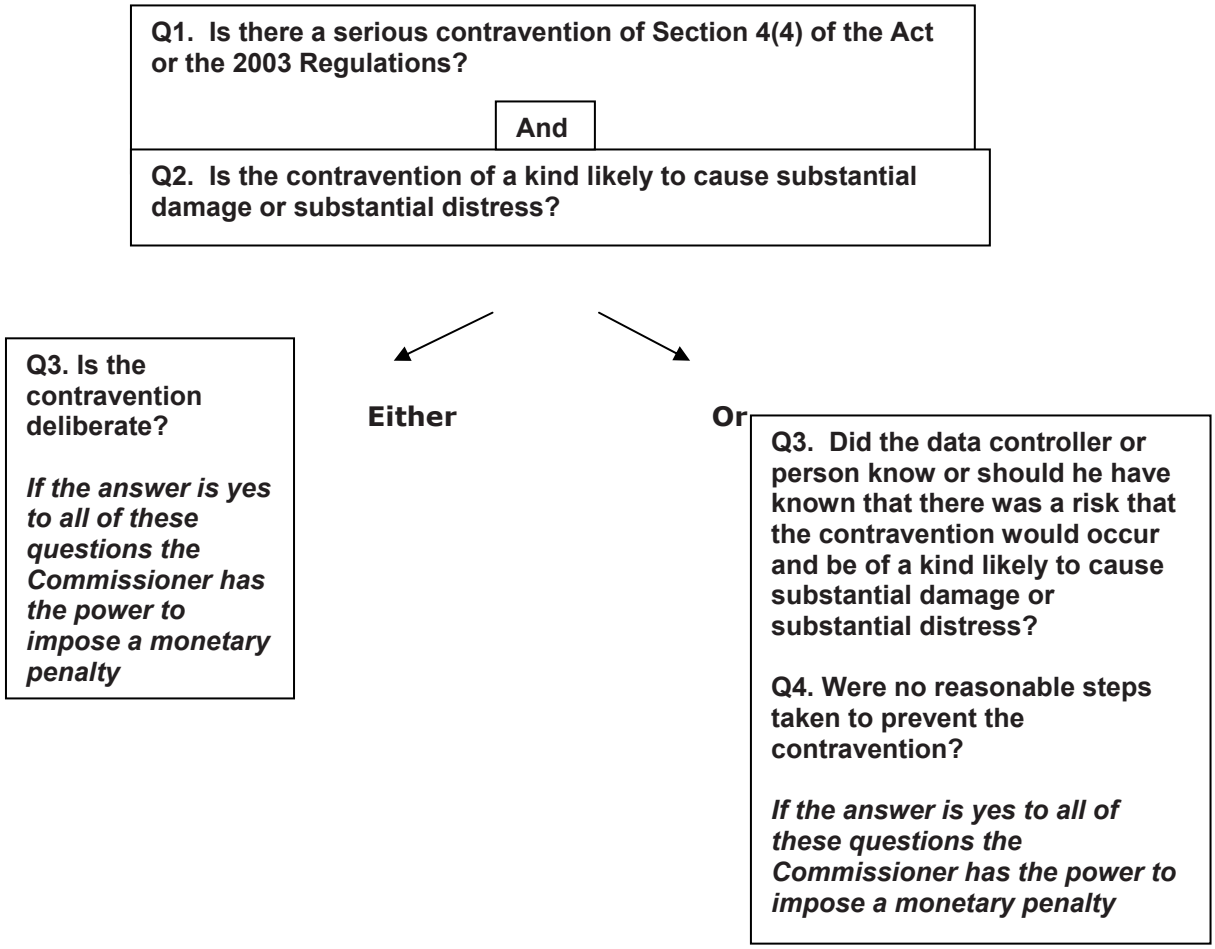
So far as the 2003 regulations are concerned the Commissioner will not approach an audit under Regulation 5B with a view to imposing a monetary penalty (other than a fixed penalty under Regulation 5C) if a breach is discovered in the process unless he has made clear beforehand that this is his intention. The Commissioner is generally of the view that such audits are a means of encouraging compliance and good practice. However, the Commissioner cannot give an absolute assurance that a monetary penalty will not be imposed following such

an audit, because he cannot rule out the need to take action where substantial risks to individuals are identified.

As a general rule a person with substantial financial resources is more likely to attract a higher monetary penalty than a person with limited resources for a similar contravention of the Act or the 2003 Regulations. For example, a monetary penalty notice was served on a sole proprietor for the sum of £1,000 following representations about his financial status. When further precedents are available from either the monetary penalty notices served by the Commissioner or the decisions of the First-tier Tribunal (Information Rights), further guidance will be produced so that those affected can better assess their position.

As a starting point the Commissioner will satisfy himself that he has the power to impose a monetary penalty in that there has been a serious contravention of the Act or the 2003 Regulations and that the other statutory requirements apply. See figure B below.

Figure B



2.1 To reiterate, the Commissioner has to be satisfied that –

a) There has been a serious contravention of section 4(4) of the Act by the data controller or the requirements of the 2003 Regulations by a person,

b) The contravention was of a kind likely to cause substantial damage or substantial distress and either,

c) The contravention was deliberate or,

d) The data controller or person knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

Commissioner's **interpretation of section 55A of the Act**

What will constitute a **serious** contravention?

The Commissioner will take an objective approach in considering whether there has been a serious contravention of the Act or the 2003 Regulations. The Commissioner will aim to reflect the reasonable expectations of individuals and society and ensure that any harm is genuine and capable of explanation. It is possible that a single breach may be sufficient to meet this threshold although evidence of multiple breaches will be more likely to amount to a serious contravention of the Act or the 2003 Regulations.

Examples – serious contravention of the Act
The failure by a data controller to take adequate security measures (use of encrypted files and devices, operational procedures, guidance etc.) resulting in the loss of a compact disc holding personal data.

Medical records containing sensitive personal data are lost following a security breach by a data controller during an office move.

Examples – serious contravention of the 2003 Regulations
Making a large number of automated marketing calls based on recorded messages or sending large numbers of marketing text messages to individuals who have not consented to receive them, particularly if distress is caused to the recipients.

Systemic failings in the processes to record and respect marketing objections which leads to an organisation persistently sending

marketing faxes to recipients who have clearly objected.

A person covertly tracks an individual's whereabouts using mobile phone location data.

What are the **reasonable steps** the Commissioner expects someone to take?

The Commissioner is more likely to consider that a person has taken reasonable steps to prevent the contravention if any of the following apply:

a) The person had carried out a risk assessment or there is other evidence (such as appropriate policies, procedures, practices or processes in place or advice and guidance given to staff) that the person had recognised the risks of handling personal data and taken steps to address them;

b) The person had good governance and/or audit arrangements in place to establish clear lines of responsibility for preventing contraventions of this type;

c) The person had appropriate policies, procedures, practices or processes in place and they were relevant to the contravention, for example, a policy to encrypt all laptops and removable media in relation to the loss of a laptop by an employee of the data controller or clear processes to screen against the Telephone Preference Service ("TPS") and their own suppression lists before making unsolicited marketing calls.

d) Guidance or codes of practice published by the Commissioner or others and relevant to the contravention were implemented by the person, for example, the person can demonstrate compliance with the BS ISO/IEC 27001 standard on information security management or that he followed the Commissioner's guidance on the 2003 Regulations.

This list is not exhaustive and the Commissioner will consider whether a person has taken reasonable steps on a case by case basis. In doing so he will take into account the resources available to the person but this alone will not be a determining factor.

Example – reasonable steps in relation to a serious contravention of the Act
In relation to a security breach the data controller rectifies a flaw in his computer systems as soon as he practicably could have done.

Example – reasonable steps in relation to a serious contravention of the 2003 Regulations
Temporarily suspending marketing operations to allow time to fix a problem when it becomes clear processes have failed, for example, because a number of calls have been made to TPS registered numbers due to a system fault.

What does the Commissioner mean by the term **substantial**?

The likelihood of damage or distress suffered by individuals will have to be considerable in importance, value, degree, amount or extent. The Commissioner will assess both the likelihood and the extent of the damage or distress objectively. In assessing the likelihood of damage or distress the Commissioner will consider whether the damage or distress is merely perceived or of real substance. The Commissioner does though consider that if damage or distress that is less than considerable in each individual case is suffered by a large number of individuals the totality of the damage or distress can nevertheless be substantial. In other words, the term substantial has a quantitative and a qualitative dimension and it is ultimately a question of fact and degree.

Example – substantial in relation to a serious contravention of the Act
Inaccurate personal data held by an ex-employer is disclosed by way of an employment reference resulting in the loss of a job opportunity for an individual.

Example – substantial in relation to a serious contravention of the 2003 Regulations
Distress caused to a large number of individuals who receive repeated automated marketing calls based on recorded messages, or marketing text messages without having given their consent, particularly where the identity of the caller or sender is concealed so stopping the messages or complaining is difficult.

What is meant by the term **damage**?

Damage is any financially quantifiable loss such as loss of profit or earnings, or other things.

Example – damage in relation to a serious contravention of the Act
Following a security breach by a data controller financial data is lost and an individual becomes the victim of identity fraud.

Example – damage in relation to a serious contravention of the 2003 Regulations
The telephone lines of a large number of organisations (including sole traders, doctor's surgeries and the emergency services) are inundated with automated marketing calls based on recorded messages or marketing text messages. Alternative arrangements have to be made so that urgent calls can be received. This results in substantial costs being incurred.

What is meant by the term **distress**?

Distress does not simply mean any injury to feelings, harm or anxiety suffered by an individual. It is really a matter of degree for the Commissioner to assess on a case by case basis. However, he will be looking for evidence that there was a significant risk that real and substantial distress would occur.

Example – distress in relation to a serious contravention of the Act
Following a security breach by a data controller medical details are stolen and an individual is tormented by the increased risk that his sensitive personal data will be made public even if his concerns do not materialise.

Example – distress in relation to a serious contravention of the 2003 Regulations
Over a period of several weeks repeated marketing calls are made or marketing text messages are sent to a vulnerable subscriber who has not agreed to receive them causing the individual to be disturbed and badly distressed by the experience.

What will constitute a **deliberate** contravention?

See section 3.4 below.

Example – deliberate in relation to a serious contravention of the Act
A marketing company collects personal data stating it is for the purpose of a competition and then, without consent, knowingly discloses the data to populate a tracing database for commercial purposes without informing the individuals concerned.

Example – deliberate in relation to a serious contravention of the 2003 Regulations
A debt collection company continues to send marketing faxes to subscribers who are registered on the Fax Preference Service ("FPS") despite their repeated objections.

A company sends marketing text messages to subscribers who have not consented to receiving them in order to encourage them to send opt-out requests to a premium rate short code.

What is meant by the term **knew or ought to have known**?

The Commissioner considers that this means a data controller or person is aware or should be aware of a risk that a contravention will occur. The test is objective and the Commissioner will expect the standard of care of a reasonably prudent person.

See section 3.4 below.

Example – knew or ought to have known in relation to a serious contravention of the Act
A data controller is warned by its IT department that employees are using sensitive personal data but fails to carry out a risk assessment or implement a policy of encrypting all laptops and removable media as appropriate.

Example – knew or ought to have known in relation to a serious contravention of the 2003 Regulations
A company that makes numerous marketing telephone calls is aware that the system it uses for blocking calls to TPS registered numbers may develop a fault but continues to make calls without assessing the likelihood of the fault occurring and the implications if it does.

3 Circumstances in which the Commissioner may consider it appropriate to issue a monetary penalty notice

3.1 The Commissioner will not impose a monetary penalty if to do so would result in the Commissioner acting inconsistently with any of his statutory duties. Nor will the Commissioner impose a monetary penalty if the contravention was discovered in the process of the Commissioner carrying out a voluntary assessment on a data controller under section 51(7) of the Act or following compliance with an assessment notice served under section 41A of the Act.

3.2 So far as the 2003 Regulations are concerned the Commissioner will not approach an audit under Regulation 5B with a view to imposing a monetary penalty (other than a fixed penalty under Regulation 5C) if a breach is discovered in the process unless he has made clear beforehand that this is his intention. The Commissioner is generally of the view that such audits are a means of encouraging compliance and good practice. However, the Commissioner cannot give an absolute assurance that a

monetary penalty will not be imposed following such audit, because he cannot rule out the need to take action where substantial risks to individuals are identified.

3.3 The Commissioner will seek to ensure that the imposition of a monetary penalty is appropriate and the amount of that penalty is reasonable and proportionate, given the particular facts of the case and the underlying objective in imposing the penalty.

3.4 In deciding whether it is appropriate to impose a monetary penalty and in determining the amount of that monetary penalty, the Commissioner will take full account of the particular facts and circumstances of the contravention and of any representations made to him.

The presence of one or more of the following factors will make the imposition of a monetary penalty more likely:

Seriousness of contravention

- The contravention is or was particularly serious because of the nature of the personal data concerned.
- The duration and extent of the contravention.
- The number of individuals actually or potentially affected by the contravention.
- The fact that it related to an issue of public importance.
- The contravention was due to either deliberate or negligent behaviour on the part of the person concerned.

Likelihood of substantial damage or substantial distress

- There was a significant risk that the contravention was of a kind (or type) to cause substantial damage or substantial distress to an individual or individuals.

Deliberate contravention

- The actions of the person which resulted in the contravention were deliberate or premeditated, for example, for financial gain.
- The person concerned was aware of and did not follow specific advice published by the Commissioner or others and relevant to the contravention.

- The contravention followed a series of similar contraventions by the person and no action had been taken to rectify the cause of the original contraventions.

Knew or ought to have known

- The likelihood of the contravention should have been apparent to a reasonably prudent person.

- The person concerned had adopted a cavalier approach to compliance and failed to take reasonable steps to prevent the contravention, for example, not putting basic security provisions in place or failing to set up any process to record objections to marketing or suppression requests from customers.

- The person had failed to carry out any sort of risk assessment and there is no evidence, whether verbally or in writing, that the person had recognised the risks of handling personal data and taken reasonable steps to address them.

- The person did not have good corporate governance and/or audit arrangements in place to establish clear lines of responsibility for preventing contraventions of this type.

- The person had no specific procedures or processes in place which may have prevented the contravention (for example, a robust compliance regime or other monitoring mechanisms).

- Guidance or codes of practice published by the Commissioner or others and relevant to the contravention, for example, the BS ISO/IEC 27001 standard on information security management or the Commissioner's guidance on the 2003 Regulations were available but had been ignored or not given appropriate weight.

Other considerations

- The need to maximise the deterrent effect of the monetary penalty by setting an example to others so as to counter the prevalence of such contraventions.

- A person had expressly, and without reasonable cause, refused to submit to a voluntary assessment or audit which could reasonably have been expected to reveal a risk of the contravention.

3.5 The presence of one or more of the following factors will make the imposition of a monetary penalty by the Commissioner less likely:

- The contravention was caused or exacerbated by circumstances outside the direct control of the person concerned and they had done all that they reasonably could to prevent contraventions of the Act or the 2003 Regulations.

  Examples
  Despite a loss of personal data by a data processor the data controller had a contract in place with a data processor and had properly monitored the data processor's compliance with the contract.

  Despite a "one-off" system error leading to an isolated breach a person can demonstrate clear processes were in place to ensure email marketing is only sent to individuals who have consented.

- The person concerned had already complied with any requirements or rulings of another regulatory body in respect of the facts giving rise to the contravention (the Commissioner will endeavour to work closely with other regulators with a view to ensuring that multiple penalties are not imposed on the same person for what is in effect a single failure).

- There was genuine doubt or uncertainty that any relevant conduct, activity or omission in fact constituted a contravention of the Act or the 2003 Regulations, although simple ignorance of the law will be no defence.

3.6 If the Commissioner considers that there are other factors, not referred to above, that are relevant to his decision whether it would be appropriate to impose a monetary penalty in a particular case, the Commissioner will explain what these are. Although there may not always be any other factors this provision allows the Commissioner to take into account circumstances that are not generally applicable but which are still relevant to the Commissioner's decision on whether or not to impose a monetary penalty in the case in question.

4 How the Commissioner will determine the amount of a monetary penalty

4.1 Once it has been decided that a monetary penalty should be imposed, the Commissioner must then consider what would be the appropriate amount, given the circumstances of the case. Again, the Commissioner will have regard to the underlying objective as set out in the Introduction and to the general approach set out in paragraphs 3.1 to 3.4 above.

4.2 A number of issues are likely to be relevant to the decision as to what would be an appropriate monetary penalty in a particular case. These issues will vary from case to case, but will be closely related to those determining whether to impose a penalty at all. One or more of the factors which may be relevant in some or all cases are described below. These factors are not exhaustive.

Nature of the Contravention

- How serious the contravention was or is in terms of the nature of the personal data concerned and the number of individuals actually or potentially affected.

- The type of individuals affected (for example, children or vulnerable adults).

- Whether the contravention was a "one-off" or part of a series of similar contraventions.

- Whether the contravention was caused or exacerbated by activities or circumstances outside the direct control of the person concerned, for example, a data processor or an errant employee.

- The duration and extent of the contravention.

- Whether guidance or codes of practice published by the Commissioner or others and relevant to the contravention were followed, for example, the BS ISO/IEC 27001 standard on information security management or Commissioner's guidance on 2003 Regulations.

The Effect of the Contravention

Whether there was, may be or might have been substantial damage or substantial distress caused to individuals.

Behavioural issues

- What procedures or processes the person had in place to avoid the contravention (for example, the robustness of their compliance regime or other monitoring mechanisms).

- What steps, if any, had been taken to avoid the contravention (for example, appropriate staff training).

- What steps, if any, the person had taken once they became aware of the contravention (for example, concealing it, voluntarily reporting it to the Commissioner, or not taking action once the Commissioner or another body had identified the contravention).

- The role of senior managers who would be expected to demonstrate higher standards of behaviour.

- Whether the person has been willing to offer compensation to those affected.

- Whether there has been any lack of co-operation or deliberate frustration, for example, failure to respond to the Commissioner's reasonable requests for information during the course of the investigation.

- Whether the person has expressly, and without reasonable cause, refused to submit to a voluntary assessment or audit which could reasonably have been expected to reveal a risk of the contravention.

Impact on the Data Controller or Person

- The Commissioner will aim to eliminate any financial gain or benefit obtained by the person concerned from non-compliance with the Act or the 2003 Regulations.

- The Commissioner will take into account the sector, for example, whether the person concerned is a voluntary organisation and also their size, financial and other resources.

- The Commissioner will consider whether liability to pay the fine will fall on individuals and if so their status (for example, charitable trustees in the voluntary sector).

- The Commissioner will consider the likely impact of the penalty on the person concerned, in particular financial and reputational impact.

- The Commissioner will take into account any proof of genuine financial hardship which may be supplied. The purpose of a monetary penalty notice is not to impose undue financial hardship on an otherwise responsible person. In appropriate cases the Commissioner will adjust the monetary penalty where, for example, a loss was made in the previous year.

Other considerations

- If the Commissioner considers that a precedent or point of principle is relevant to a decision in a particular case, the Commissioner will explain that relevance.

- If the Commissioner considers there are other factors, not referred to above, that are relevant in a particular case to his determination of the amount of the monetary penalty the Commissioner will explain what these are. Although there may not always be any other factors this provision allows the Commissioner to take into account circumstances that are not generally applicable but which are still relevant to the Commissioner's determination of the amount of a monetary penalty in the case in question.

4.3 Having considered the relevant factors in relation to the particular facts and circumstances of the contravention under consideration, the Commissioner will determine the level of the monetary penalty.

5 Notice of intent

5.1 The amount of the monetary penalty determined by the Commissioner must not exceed £500,000. Once the level of a monetary penalty has been determined, the Commissioner must serve a notice of intent before he can issue a monetary penalty notice. The notice of intent will set out the proposed amount of the monetary penalty.

5.2 A notice of intent must inform the recipient that he may make written representations in relation to the Commissioner's proposal within a period specified in the notice, and contain such other information as is prescribed in the Data Protection (Monetary Penalties)(Maximum Penalty and Notices) Regulations 2010.

5.3 A notice of intent must contain the following information:

(a) the name and address of the data controller or person;

(b) the grounds on which the Commissioner proposes to serve a monetary penalty notice, including -

(i) the nature of the personal data involved in the contravention;

(ii) a description of the circumstances of the contravention;

(iii) the reason the Commissioner considers that the contravention is serious;

(iv) the reason the Commissioner considers that the contravention is of a kind likely to cause substantial damage or substantial distress;
and

(v) whether the Commissioner considers that section 55A(2) applies, or that section 55A(3) applies, and the reason the Commissioner has taken this view;

(c) an indication of the amount of the monetary penalty the Commissioner proposes to impose and any aggravating or mitigating features the Commissioner has taken into account; and

(d) the date on which the Commissioner proposes to serve the monetary penalty notice.

5.4 The notice of intent must specify a period within which written representations can be made to the Commissioner. This period must be a reasonable period and must not be less than 21 days beginning with the first day after the date of service of the notice of intent.

6 Provision to make representations to the Commissioner before a final decision is made

6.1 The purpose of the notice of intent is to set out the Commissioner's proposal and enable the recipient to make representations to the Commissioner's office. The recipient may wish to comment on the facts and views set out by the Commissioner in the notice of intent or to make general remarks on the case and enclose documents or other material such as

details of their finances. For example, if a security breach was caused entirely by the actions of a data processor, a data controller may want to provide the Commissioner with a full explanation of the circumstances that led to the breach together with a copy of the contract between the data controller and the data processor and the steps taken by the data controller to ensure compliance with the security guarantees in the contract. The recipient of the notice should also inform the Commissioner if any confidential or commercially sensitive information should be redacted from a monetary penalty notice.

6.2 The Commissioner must consider any written representations made in relation to a notice of intent when deciding whether to serve a monetary penalty notice. Following expiry of the period referred to in paragraph 5.4 above, the Commissioner will take the following steps:

a) reconsider the amount of the monetary penalty generally, and whether it is a reasonable and proportionate means of achieving the objective or objectives which the Commissioner seeks to achieve by this imposition;

b) ensure that the monetary penalty is within the prescribed limit of £500,000; and

c) ensure that the Commissioner is not, by imposing a monetary penalty, acting inconsistently with any of his statutory duties and that a monetary penalty notice will not impose undue financial hardship on an otherwise responsible person.

6.3 Having taken full account of any representations and any other circumstances relevant to the particular case under consideration, the Commissioner will decide whether or not to impose a monetary penalty and, if so, determine an appropriate and proportionate monetary penalty. The monetary penalty should not be substantially different to the amount proposed in the Notice of Intent unless the representations of the data controller or person can justify a reduction.

6.4 The Commissioner must either serve a monetary penalty notice or a cancellation notice relating to the notice of intent within a reasonable period following expiry of the period referred to in paragraph 5.4 above. The Commissioner may not serve a monetary penalty notice if a period of 6 months has elapsed after the service of the notice of intent.

7 Monetary penalty notice

7.1 The Commissioner may serve a monetary penalty notice on a data controller or person requiring them to pay a monetary penalty of an amount determined by the Commissioner and specified in the monetary penalty notice. The monetary penalty notice must contain such information as is prescribed in the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010.

7.2 A monetary penalty notice must contain the following information:

(a) the name and address of the data controller or person;

(b) details of the notice of intent served;

(c) whether the Commissioner received written representations following the service of the notice of intent;

(d) the grounds on which the Commissioner imposes the monetary penalty, including-

(i) the nature of the personal data involved in the contravention;

(ii) a description of the circumstances of the contravention;

(iii) the reason the Commissioner is satisfied that the contravention is serious;

(iv) the reason the Commissioner is satisfied that the contravention is of a kind likely to cause substantial damage or substantial distress; and

(v) whether the Commissioner is satisfied that section 55A(2) applies, or that section 55A(3) applies, and the reason the Commissioner is so satisfied;

(e) the reasons for the amount of the monetary penalty including any aggravating or mitigating features the Commissioner has taken into account when setting the amount;

(f) details of how the monetary penalty is to be paid;

(g) details of, including the time limit for, the right of appeal of the data controller or person against:

(i) the imposition of the monetary penalty, and
(ii) the amount of the monetary penalty; and

(h) details of the Commissioner's enforcement powers under section 55D.

7.3 The monetary penalty notice will be published on the Commissioner's website with any confidential or commercially sensitive information redacted. The monetary penalty must be paid to the Commissioner by BACS transfer or cheque within the period specified in the monetary penalty notice which will be a period of at least 28 calendar days beginning with the first day after the date of service of the monetary penalty notice. The monetary penalty is not kept by the Commissioner but must be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

Early payment discount

7.4 If the Commissioner receives full payment of the monetary penalty within 28 calendar days of the monetary penalty notice being served, the Commissioner will reduce the monetary penalty by 20%. However, this early payment discount will not be available if a data controller or person decides to exercise their right of appeal to the First-tier Tribunal (Information Rights).

Variation of a monetary penalty notice

7.5 The Commissioner may serve a variation notice. A variation notice is a notice that the Commissioner proposes to vary a monetary penalty notice.
A variation must -

a) identify the notice concerned;

b) specify how the notice is to be varied; and

c) specify the date on which the variation is to take effect.

Any notice of variation of the monetary penalty notice will be published on the Commissioner's website with any confidential or commercially sensitive information redacted.

The variation notice must extend the period of time by which a monetary penalty is to be paid if it is reasonable in all the circumstances to do so.

Enforcement of a monetary penalty notice

7.6 The Commissioner must not take action to enforce a monetary penalty unless:

(a) the period specified in the monetary penalty notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;

(b) all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and

(c) the period for the data controller or person to appeal against the monetary penalty and any variation of it has expired.

7.7 In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Cancellation of a monetary penalty notice

7.8 The Commissioner can cancel a monetary penalty notice by serving a cancellation notice. A cancellation notice is a notice that a monetary penalty notice ceases to have effect. A cancellation notice must-

(a) identify the notice concerned;

(b) state that the notice concerned has been cancelled; and

(c) state the reasons for the cancellation.

Any notice of cancellation of the monetary penalty notice will be published on the Commissioner's website with any confidential or commercially sensitive information redacted.

8 Right of Appeal against monetary penalty notice

8.1 A data controller or person on whom a variation notice or monetary penalty notice is served may appeal to the First-tier Tribunal (Information Rights) against a variation notice or the issue of the monetary penalty notice and/or the amount of the penalty specified in the notice. Please refer to Her Majesty's Court and Tribunal Service at www.mailto:justice.gov.uk for the appeals procedure. Each monetary penalty notice will specify the period within which either the financial penalty must be paid or an appeal must be lodged.

ISBN 978-1-4741-1711-1