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

December 2015

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 9781474126519
Web ISBN 9781474126526

ID 04121508 12/15 52879 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 issuing of monetary penalties

Data Protection Act 1998
Privacy and Electronic Communications Regulations 2003

Contents

Introduction

1. This guidance sets out the circumstances in which the Information Commissioner (the "Commissioner") will consider it appropriate to issue a monetary penalty notice under the Data Protection Act 1998 (the "DPA") or Privacy and Electronic Communication Regulations ("PECR"). It also explains how he will determine the amount of the penalty.

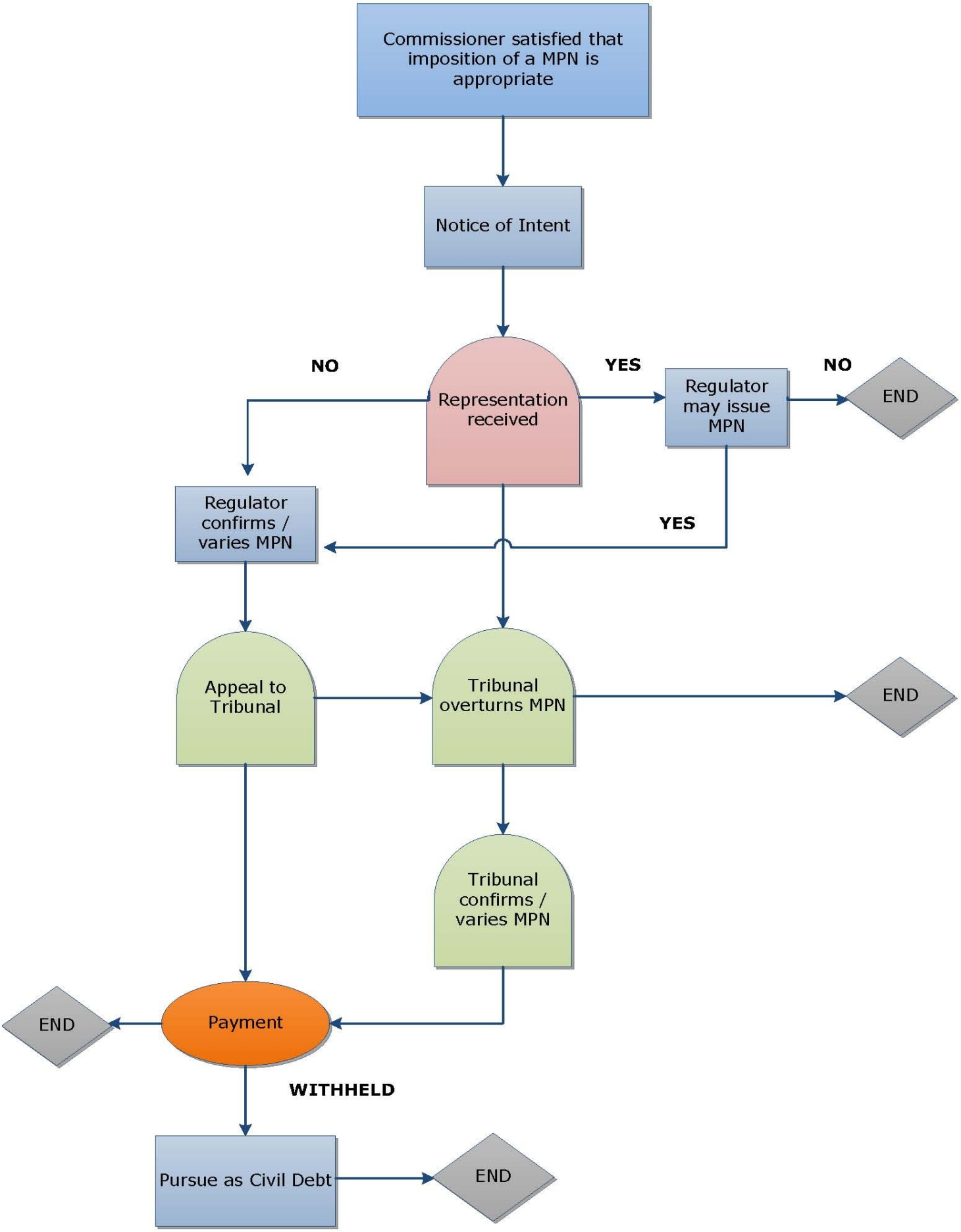
2. It should be read in conjunction with the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

3. This is the statutory guidance issued under the DPA. This means that the Secretary of State has been consulted and it has been laid before Parliament.

4. The Commissioner will consider altering or replacing this guidance in the way provided for in the DPA 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.

Overview

- The Commissioner's objective in imposing a monetary penalty is to promote compliance with the DPA or with PECR.
- The amount of the monetary penalty determined by the Commissioner cannot exceed £500,000. It 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.
- The Commissioner will take into account the sector, size, and financial and other resources of a data controller or person, as it is not the purpose of a penalty notice to impose undue financial hardship on an otherwise responsible person.
- Where the Commissioner intends to issue a monetary penalty notice he will first serve a 'notice of intent'. This will specify the proposed amount of the penalty and the period within which the recipient can make written representations 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.
- If the Commissioner proposes to vary the amount of the monetary penalty, then he must issue a variation notice which identifies the monetary penalty notice concerned, specifies how the notice is to be varied; and specifies the date on which the variation is to take effect.
- 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 that notice and/or the amount of the penalty specified in the notice.


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

5. To serve a monetary penalty notice for a breach of the DPA, the Commissioner must be satisfied that -

   - there has been a serious contravention of Section 4(4) of the DPA by the data controller,

   - the contravention was of a kind likely to cause substantial damage or substantial distress; and **either**,

   - the contravention was either deliberate; **or**,

   - the data controller 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.

6. Following the introduction of the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2015, there is no longer a requirement to demonstrate substantial damage and substantial distress in PECR cases.

7. Therefore, in order to serve a monetary penalty notice under PECR, the Commissioner need only be satisfied that;

   - There has been a serious contravention of the requirements of PECR by a person,

   - the contravention was deliberate; **or**,

   - the person knew, or ought to have known, that there was a risk that the contravention would occur, but failed to take reasonable steps to prevent the contravention.

8. 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.

9. Monetary penalty notices are only designed to deal with serious contraventions of the DPA and PECR. 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.

10. 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 promote understanding of the DPA and PECR where possible, in order to make it easier for organisations to comply with their obligations under both the DPA and PECR.

11. 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 PECR in question.

12. 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 PECR.

Who can be subject to a monetary penalty?

13. The DPA and PECR apply to the whole of the UK. 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 DPA, carry out a voluntary assessment under section 51(7) of the DPA, serve an assessment notice under section 41A of the DPA or carry out an audit under PECR as amended.

    The monetary penalty is not kept by the Commissioner, but must be paid into the Consolidated Fund owned by HM Treasury.

14. In relation to serious contraventions of the DPA 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.

15. 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 DPA 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.

16. In relation to serious contraventions of the requirements of PECR 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.

17. 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 DPA or PECR.

18. 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.

The statutory threshold for a monetary penalty

The meaning of 'Serious contravention'

19. The Commissioner will take an objective approach in considering whether there has been a serious contravention of the DPA or PECR. The Commissioner will aim to reflect the reasonable expectations of individuals and society and ensure that any harm is genuine and capable of explanation.

20. It is possible that a single breach may be sufficient to meet this threshold although evidence of multiple breaches and systemic non-compliance will be more likely to amount to a serious contravention of the DPA or PECR.

Examples – serious contravention of the DPA

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 and no policies or procedures were in place to protect the personal data.

Examples – serious contravention of PECR

Making a large number of automated marketing calls based on recorded messages or sending large numbers of marketing text messages or emails to individuals who have not consented to receive them.

Making a large number of live marketing calls to consumers

who have subscribed to the TPS.

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

The meaning of 'likely to cause substantial damage or substantial distress

21. In relation to contraventions of the DPA, but not PECR, the Commissioner must be satisfied that the contravention is of a kind likely to cause substantial damage or distress.

The meaning of 'likely'

22. In ICO vs Niebel, *[2014] UKUT 225 (AAC), (11 June 2014),* (a monetary penalty appeal case), the Upper Tribunal endorsed the definition of 'likely' used by Mr Justice Munby in the case of *(Lord) v Secretary of State for the Home Department [2003] EWHC 2073 (Admin)* (a DPA case).

23. Judge Wikeley said;

'…According to Munby J, "likely" meant something more than "a real risk", ie a significant risk, "even if the risk falls short of being more probable than not"…The tribunal here agreed, noting that whereas the balance of probabilities test "is designed to produce just one outcome whereas, as a matter of common experience, an event can have more than one 'likely outcome'". I also agree with that analysis.' (Para 27)

24. On the basis of these judgements, 'likely' denotes more than just a hypothetical or remote possibility; rather, there must have been a real and significant risk that the contravention was of a kind (or type) likely to cause substantial damage or substantial distress to an individual or individuals.

The meaning of 'substantial'

25. The term 'substantial' is not defined in the Act and should be given its ordinary dictionary meaning.

26. The Commissioner does 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 qualitative dimension and it is ultimately a question of fact and degree.

The meaning of 'damage'

27. 'Damage' may be defined as any financially quantifiable loss such as loss of profit or earnings, or other things.

> **Example**
>
> 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**
>
> Following a security breach by a data controller financial data is lost and an individual becomes the victim of identity fraud.

The meaning of 'distress'

28. '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**
>
> 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.

The meaning of 'a deliberate' contravention'

29. A deliberate contravention means carrying out a deliberate act that contravenes the DPA or PECR.

30. It isn't necessary for a data controller or person to have known that they were breaking the law for the contravention to be considered 'deliberate'. Similarly, it won't be a defence for a data controller or person to claim they weren't aware that the contravention broke the law.

Example – deliberate in relation to a serious contravention of the DPA

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 PECR

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.

The meaning of 'knew or ought to have known'

31. 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.

Example – knew or ought to have known in relation to a serious contravention of the DPA

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 PECR

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.

The meaning of 'reasonable steps'

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

a) The person had carried out a risk assessment, such as a privacy impact 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 PECR.

33. 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 DPA

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 DPA

The data controller loses a USB stick containing sensitive personal information, but had taken the precaution of encrypting all the data on the device.

Example – reasonable steps in relation to a serious contravention of PECR

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.

The Commissioner's aim in imposing a monetary penalty

34. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA or with PECR.

35. The 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.

36. This applies both in relation to the specific type of contravention and other contraventions more generally. Here, the Commissioner will have regard to the general approach set out in paragraphs 42 to 46 below.

37. 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.

Factors the Commissioner will take into account when deciding whether to issue a monetary penalty notice.

38. 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 specific facts and circumstances of the contravention and of any representations made to him.

39. In particular, the Commissioner will consider whether one or more of the following factors are present.

Seriousness of the contravention

40. The Commissioner will be more likely to issue a penalty if;

- the contravention is, or was, particularly serious because of the nature of the personal data concerned.
- a significant number of individuals have, or could potentially be, affected by the contravention.
- the contravention relates to an issue of public importance.
- the contravention was due to either deliberate or negligent behaviour on the part of the person concerned.

In addition, the Commissioner will also take the extent and duration of the contravention into consideration.

Example

On 15 October 2013 the Commissioner issued a monetary penalty notice to North East Lincolnshire County Council for a contravention of Principle 7 of the DPA.

The Council had lost an unencrypted memory device containing personal data and sensitive personal data relating to 286 children.

In addressing the seriousness of the contravention, the Commissioner cited the nature of the data and the Council's failure to take appropriate steps to safeguard the information against accidental loss;

'*In particular, in this case, the data controller has failed to take sufficient appropriate technical and organisational measures against accidental loss of personal data such as a combination of, training staff on the importance of using encrypted USB sticks; technical controls to prevent downloading on to unencrypted portable media; effective organisational policies and controls; and enabling compliance with those policies and controls. The Commissioner considers that the contravention is serious because the measures did not ensure a level of security appropriate to the nature of the data to be protected and the harm that might result from accidental loss*.' (Para 23)

Substantial damage and distress (DPA only)

41. The 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 extent of damage or distress the Commissioner will consider whether the damage or distress is merely perceived or of real substance.

Example

On 31 October 2014 the Commissioner issued a monetary penalty notice to Worldview Limited for a contravention of Principle 7 of the DPA.

This was after a vulnerability on the company's website had allowed attackers to access the full payment card details of 3,814 customers.

The Commissioner determined that this contravention could cause substantial damage to the data subjects because of its potential to be used for fraudulent purposes;

'*Active card data was obtained over a 10 day period including the CVV values that could have been decrypted. Although there is no evidence of fraud having taken place as a result of this incident, the personal data that was obtained was clearly of interest to the attacker given the targeted nature of the attack, and could still be used for fraudulent purposes. It is reasonable to assume therefore that it is likely that the attacker would use this information in a manner that would cause substantial damage to the data subjects either in the short or long term*.' (Page 5)

The Commissioner also concluded that the data subjects would be likely to suffer distress from the knowledge that their information had fallen into the hands of unauthorised parties.

'*The data subjects would also be likely to suffer from substantial distress on being informed that their personal data had been accessed by an unauthorised third party and could have been further disclosed even though, so far as the Commissioner is aware, there has been no evidence of fraudulent transactions being conducted as a result of this incident. The knowledge of this access alone is likely to cause substantial distress*.' (Page 5)

Deliberate contravention

42. The Commissioner will be more likely to issue a penalty if;

- 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) that was 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.

Example

On 2 December 2014 the Commissioner issued a monetary penalty notice to Parklife Manchester Limited for a contravention of Regulation 23 of PECR in connection with the sending of unsolicited text messages.

The texts in question were sent to 70,000 people who had purchased tickets for the Parklife Weekender event, and appeared on the recipients' mobile phone to have been sent by "Mum".

The penalty notice pointed to the fact that the Commissioner has published detailed guidance explaining the circumstances in which organisations can carry out electronic marketing. This guidance specifically states that organisations must not disguise or conceal their identity in marketing texts and emails.

The Commissioner went on to conclude that Parklife had purposely disguised or concealed its identity, and that its contravention of PECR was deliberate.

The data controller knew or ought to have known about the risk of a contravention

43. The Commissioner will be more likely to issue a penalty if;

- 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 PECR were available but had been ignored or not given appropriate weight.

Example

On 21 July 2014 the Commissioner issued a monetary penalty notice to Think W3 Limited for a contravention of Principle 7 of the DPA. This followed an incident in which a hacker succeeded in gaining access to the customer payment card data of its wholly owned subsidiary company, Essential Travel Limited.

The Commissioner was satisfied that Think W3 should have known about the risk of a contravention. He observed;

'The data controller should have been aware of the risks associated with any compromise of payment card and cardholder data due to the nature of the data being collected. By 2011 the data controller was aware of a number of issues with its Payment Card industry – Data Security standard compliance which caused it to review some of its security practices. However, the data controller was slow in implementing improvements to its systems (partly as a result of external factors)'

'In the circumstances, the data controller knew or ought to

*have known that there was a risk that the contravention would occur…' (*Page 6)

The data controller or person failed to take 'reasonable steps'

44. This meaning of 'reasonable steps' is defined in paragraph 32 of the guidance. The Commissioner is more likely issue a monetary penalty in cases where a data controller or person has neglected to take such steps, for example;

- failing to implement adequate information policies and procedures, or failing to put protocols in place to check the effectiveness of those procedures;
- failing to provide management and staff with sufficient training;
- failing to take appropriate security measures, such as encrypting personal information on portable devices like laptops and USB sticks, or not locking paper documents away securely.
- using a data processor that didn't provide sufficient guarantees that it had appropriate technical and organisational security measures in place
- failing to cross check the numbers on a telephone marketing list against the numbers on the TPS.

Example

On 15 October 2013 the Commissioner issued a monetary penalty notice to North East Lincolnshire Council for a contravention of Principle 7 of the DPA. The case concerned the loss of a USB stick containing personal and sensitive personal data.

Amongst the factors cited in the Commissioner's penalty notice was a lack of staff training and inadequate organisational policies and controls.

'The data controller did not take reasonable steps to prevent the contravention such as a combination of training staff on the importance of using encrypted USB sticks; technical controls to prevent downloading on to unencrypted portable media; effective organisational policies and controls; and enabling compliance with those policies and controls.' (Para 26 viii)

Example

On 5 July 2013 the Commissioner issued a monetary penalty notice to Tameside Energy Services for making unsolicited marketing calls in contravention of Regulation 21 of PECR.

The Commissioner was of the view that the company had failed to take reasonable steps to prevent the contravention because its procedures for checking telephone numbers against the TPS were ineffective. He stated;

'Tameside is a company which had been in existence since 2003 and has been operating under these regulations since then. Tameside's business is heavily reliant upon direct marketing to consumers. It is a fundamental requirement of the PECR that TPS registered numbers have to be suppressed and that consent is required from consumers who are TPS registered before marketing calls can be made to them.

Tameside has provided no evidence of any formal policies and procedures in place for the staff to follow to ensure they know how to comply with PECR. Tameside should have been able to demonstrate that they had effective systems in place to prevent the breaches of PECR.

Tameside said they had purchased a daily TPS list for it to use but it was not being used effectively so as to prevent PECR breaches.' (Paras 57, 58 and 59)

45. For more examples of DPA and PECR monetary penalty notices served by the Commissioner, please see the Enforcement pages of the ICO website.

Factors that will make the imposition of a penalty less likely

46. 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 DPA or PECR.

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 DPA or PECR, although simple ignorance of the law will be no defence.

47. 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.

48. 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.

Other considerations

49. In deciding whether or not to impose a penalty, the Commissioner may also take into account;

- 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.

- Whether 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.

50. The Commissioner will not impose a monetary penalty if to do so would result in him acting inconsistently with any of his statutory duties. The DPA does not allow the Commissioner to impose a monetary penalty for serious contraventions of the DPA 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 DPA or following compliance with an assessment notice served under section 41A of the DPA.

51. So far as PECR 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.

52. 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.

Additional factors the Commissioner will take into account in determining the amount of the monetary penalty

53. 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.

54. 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.

55. In determining the amount, the Commissioner will have regard to the underlying objectives set out in paragraphs 36 to 39 and the general approach set out in paragraphs 42 to 46.

56. He may also take the additional factors listed below into consideration, when relevant (this list is not intended to be exhaustive).

- 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.

- 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 data controller or 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 data controller or 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 DPA or PECR.

- 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.

57. 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.

Notice of intent

58. The amount of the monetary penalty determined by the Commissioner must not exceed £500,000. Once the level of a monetary penalty has been decided, 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.

59. 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.

60. 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) in respect of a contravention of the Act, 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.

61. 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.

Representations to the Commissioner

62. 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.

63. 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.

64. 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 63 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.

65. 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.

66. The Commissioner must either serve a monetary penalty notice or write to the data controller or person advising that no further action is to be taken in regard to the contravention specified in the notice of intent. 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.

Information to be included in a monetary penalty notice

67. 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.

68. 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) in respect of a contravention of the Act, 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.

69. 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.

70. 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

71. If the Commissioner receives full payment of the monetary penalty within 28 calendar days of the monetary penalty notice being sent, 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

72. The Commissioner may serve a variation notice. A variation notice is a notice that the Commissioner proposes to vary a monetary penalty notice. It 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.

73. 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.

74. 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

75. 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.

76. 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

77. 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.

78. 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.

Right of Appeal against a monetary penalty notice

79. 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 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 978-1-4741-2651-9