Information Commissioner's Office

Draft

Statutory guidance on our PECR powers

Pursuant to our obligations under s55C DPA 1998

ico.
Information Commissioner's Office

Contents

Foreword

We will insert a foreword here in the final version of the statutory guidance.

About this guidance

What is the purpose of this guidance?

The mission of the Information Commissioner's Office (ICO) is to uphold information rights for the UK public in the digital age. This statutory guidance on our PECR powers sits alongside our regulatory action policy and our statutory guidance on our regulatory action, which together set out how the ICO carries out this mission.

We are issuing this statutory guidance to comply with our obligations under section 55C of the Data Protection Act 1998 (DPA 1998). It specifically deals with our powers to serve a monetary penalty notice (MPN) on a person or organisation or an officer of a body for data protection failures in respect of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). This guidance replaces the 'Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the DPA 1998'. These provisions of the DPA 1998 remain in force for the purposes of PECR, even with the introduction of the DPA 2018.

In line with our statutory obligations, this document's purpose is to provide clarity to those we regulate and the public about our approach to exercising these regulatory powers.

What does the guidance cover?

Section 55C of the DPA 1998 requires us to prepare and issue guidance on how we propose to exercise our powers under section 55A of the DPA 1998. The guidance must deal with:

- the circumstances in which we would consider it appropriate to issue a monetary penalty notice under PECR; and
- how we determine the amount of the penalty.

What doesn't the guidance cover?

This guidance does not cover our data protection responsibilities under the Data Protection Act 2018 (DPA 2018). Our obligations for guidance under that legislation can be found in the accompanying statutory guidance on our regulatory action document.

Who is this guidance for?

This guidance is to inform all those who collect, use, store and share information about our statutory powers to issue monetary penalty notices under the UK's PECR legislation.

Which statutory obligation does the publication of this guidance fulfil?

By issuing this document, we are fulfilling our statutory obligations to issue guidance as to how we propose to exercise our powers in respect of imposing monetary penalties, together with the accompanying procedural rights (sections 55C DPA 1998).

What is the status of this guidance?

We must produce guidance on how we use our statutory powers. Following our obligations set out in section 55C (DPA 1998), in producing this document we consulted with ICO colleagues and ran a formal consultation with the public. We carefully considered the outcome of this consultation and made appropriate amendments to this policy before we shared it with Parliament for approval. We will keep this guidance under review to ensure it remains relevant and accurate.

Further reading

PLACEHOLDER Statutory guidance on our regulatory action

PLACEHOLDER Regulatory action policy (RAP)

Data Protection Act 1998 (legislation.gov.uk)

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (legislation.gov.uk)

Monetary penalty notices (section 55A DPA 1998)

What is a monetary penalty notice (MPN)?

Monetary penalty notices (MPNs) are specific to contraventions of PECR. They should not be confused with penalty notices as described in our statutory guidance on our regulatory action (which is terminology relevant to the DPA 2018).

Under section 55A of the DPA 1998, where we see a serious contravention of PECR, we can serve an MPN on a person or organisation.

An MPN is a formal document that we issue (under section 55A of the DPA 1998) when we intend to fine a person or organisation for a breach, or breaches, of PECR. The MPN sets out the amount we intend to fine and the reasons for our decision.

When would we issue an MPN?

Our aim in applying MPNs is to ensure compliance with PECR and UK information rights obligations. To do this, penalties must provide an appropriate sanction for any breach of data protection legislation and act as an effective, proportionate deterrent to future non-compliance.

When would an MPN be appropriate?

We have the power to serve an MPN on a person or organisation, if we are satisfied that:

- a **serious contravention** of PECR occurred; and
- the contravention was **deliberate**; or
- the person or organisation **knew or ought to have known** that there was a risk that the contravention would occur but failed to take **reasonable steps** to prevent it.

The contravention must also be **likely to cause substantial damage or distress**, other than for breaches of Regulations 19-24 of PECR, where this requirement does not apply.

What do we mean by 'serious contravention'?

We take an objective approach in considering whether a person or organisation commits a serious contravention of PECR. We aim to reflect the reasonable expectations of the public and ensure that any harm is genuine and that we can clearly explain it. We may consider the following to be serious contraventions:

- A company, looking to increase their customer base, decides to obtain an electronic copy of the telephone directory. They then decide to call each listed number, without checking their own 'do not call' list or screening the numbers against the Telephone Preference Service (TPS) register.
- A company engages in the sequential dialling of hundreds, thousands or millions of numbers, without screening against their own 'do not call' list or the TPS register.
- A company purchases hundreds or thousands of people's personal data, including telephone numbers, from a third-party data broker. They use the telephone numbers to make automatic marketing calls to those people.

It is possible that a single breach may be sufficient to meet this threshold. However, evidence of multiple breaches and systemic non-compliance is more likely to amount to a serious contravention of PECR.

We are more likely to issue an MPN if the contravention:

- is, or was, particularly serious because of the nature of the personal data concerned. For example, special category data;
- did affect, or could potentially affect a significant number of people;
- relates to an issue of public importance; or
- was due to either deliberate or negligent behaviour on the part of the person or organisation concerned.

In addition, we take into account the extent and duration of the contravention.

Examples of serious contraventions of PECR may be where a person or organisation:

- makes a large number of automated marketing calls based on recorded messages or sends large numbers of marketing text messages or emails to people who did not give their consent to receive them;
- makes a large number of live marketing calls to consumers who subscribed to the TPS; or
- covertly tracks another individual's whereabouts using mobile phone location data.

What do we mean by a 'deliberate' contravention?

A deliberate contravention means carrying out a premeditated act or course of action that contravenes PECR. A person or organisation does not have to know that they were breaking the law for us to consider the contravention 'deliberate'. Similarly, it is not a defence for a person or organisation to claim they were not aware that the contravention broke the law.

We are more likely to issue a penalty if:

- the person or organisation's actions which resulted in the contravention were deliberate or premeditated, for example, for financial gain;
- the person or organisation concerned was aware of and did not follow specific advice published by us (or others) that was relevant to the contravention; or
- the contravention followed a series of similar contraventions by the person or organisation and they took no action to rectify the cause of the original contraventions.

Examples of deliberate PECR contraventions:

- A company makes automated calls to a list of bought in numbers. The director sets up the dialler so that it does not display a calling number, the relayed message does not identify who is calling and does not give any way to contact the organisation.
- A company sends marketing text messages to subscribers who have not consented to receiving them. This encourages them to send opt-out requests to a premium rate short code.

What do we mean by 'knew or ought to have known'?

This means the person or organisation is aware or should be aware of a contravention risk. The test is objective and we expect the standard of care of a reasonably prudent person or organisation.

We are more likely to issue a penalty if the person or organisation:

- would have known the likelihood of the contravention or it would be apparent to a reasonably prudent person;
- adopted a careless approach to compliance and failed to take reasonable steps to prevent the contravention, eg by not putting basic security provisions in place or failing to set up any process to record customer objections to marketing or suppression requests;
- failed to carry out any sort of risk assessment and did not recognise the risks of handling personal data or take reasonable steps to address them;
- did not have good corporate governance or audit arrangements in place to establish clear lines of responsibility for preventing contraventions of this type;
- had no specific procedures or processes in place which may have prevented the contravention (for example, a robust compliance regime or other monitoring mechanisms); or
- ignored or did not give appropriate weight to guidance or codes of practice published by us or others and relevant to the contravention (for example, the BS ISO/IEC 27001 standard on information security management or our guidance on PECR).

An example of a situation where a person or organisation knew or ought to have known of a serious PECR contravention:

- A company makes numerous marketing telephone calls. They are aware that the system they use for blocking calls to TPS-registered numbers may develop a fault. However, they continue to make calls without assessing the likelihood of the fault occurring and the implications if it does.

What do we mean by 'reasonable steps'?

We are more likely to consider that a person or organisation took 'reasonable steps' if any of the following apply:

- A risk assessment, such as a data protection impact assessment (DPIA) or other evidence (appropriate policies, procedures, practices or processes in place or advice and guidance given to staff) shows that the person or organisation recognised the risks of handling personal data and took steps to address them.
- The person or organisation has good governance and audit arrangements in place to establish clear lines of responsibility for preventing contraventions of this type.
- The person or organisation has appropriate policies, procedures, practices or processes in place and they were relevant to the contravention, for example, clear processes to screen against the TPS and their own suppression lists before making unsolicited marketing calls.
- The person or organisation implements ICO (or others) guidance or codes of practice relevant to the contravention. For example, the person or organisation demonstrates compliance with the BS ISO/IEC 27001 standard on information security management or that they follow our PECR guidance.

This list is not exhaustive and we consider whether a person or organisation took reasonable steps on a case-by-case basis. In doing so, we take into account the resources available, but this alone is not a determining factor.

An example of reasonable steps taken in response to a serious contravention of PECR:

- A business temporarily suspends marketing operations to allow time to fix a problem, when it becomes clear a number of calls were made to TPS-registered numbers due to a system fault.

We are more likely to issue a monetary penalty in cases where a person or organisation failed to:

- implement adequate information policies and procedures or failed to put protocols in place to check their effectiveness;

- provide sufficient training to management and staff;
- take appropriate security measures, such as encrypting personal information on portable devices like laptops and USB sticks, or not locking paper documents away securely; or
- use a data processor with sufficient guarantees that they had appropriate technical and organisational security measures in place to cross check the numbers on a telephone marketing list against the numbers on the TPS.

What do we mean by 'likely to cause substantial damage or distress'?

Other than for breaches of Regulations 19-24 of PECR, the contravention must be likely to cause substantial damage or distress.

- 'Likely' means more than just a hypothetical or remote possibility. There must have been a real and significant risk that the contravention would cause substantial damage or substantial distress.
- 'Substantial' is given its ordinary dictionary meaning and will depend on the facts. It can mean a considerable amount of damage or distress to one person, or less than considerable damage or distress to many people.
- 'Damage' can include any financially measurable loss, such as loss of profit or earnings. For example if, following a security breach, a person has their financial data stolen and then becomes an identity fraud victim.
- 'Distress' can include any injury to feelings, harm or anxiety that a person suffers. We assess this on a case-by-case basis. For example, if a person has their medical details stolen following a security breach, they may be tormented by the thought of those medical details being made public, even if this does not happen.

What factors make us less likely to impose a penalty?

The presence of one or more of the following factors makes us less likely to impose a monetary penalty:

- Circumstances outside of the direct control of the person or organisation caused or exacerbated the contravention. They did all that they reasonably could to prevent contraventions of PECR.
- The person or organisation concerned already complied with any requirements or rulings of another regulatory body in respect of the facts giving rise to the contravention.
- There was genuine doubt or uncertainty that any relevant conduct, activity or omission in fact constituted a contravention of PECR, although simple ignorance of the law is no defence.

What other considerations would we take into account?

In deciding whether or not to impose a penalty, we may also take into account:

- the need to maximise the monetary penalty's deterrent effect, by setting an example to others so as to counter the prevalence of such contraventions; or
- whether the person or organisation expressly, and without reasonable cause, refused to submit to a voluntary assessment or audit which could reasonably have revealed a risk of the contravention.

If we consider that there are other factors, not referred to above, that are relevant to our decision whether or not to impose an MPN in a particular case, we would explain what these are.

Officer penalties (section 55A(3B) DPA 1998)

What is an officer penalty?

Under section 55A of the DPA 1998 (and through PECR 2018) we can serve an MPN on an Officer (eg a director or manager) of a Body (a body corporate or Scottish partnership) where there has been a serious contravention of Regulations 19-24 of PECR. Section 55A(3C) of the DPA 1998 defines the terms 'Officer' and 'Body'.

An MPN is a formal document that we issue (under section 55A of the DPA 1998 and through PECR 2018) when we intend to fine an Officer for a breach, or breaches of Regulations 19-24 of PECR. The MPN sets out the amount we intend to fine and the reasons for our decision.

We can serve an MPN on an Officer if:

- we also serve an MPN on the Body where the individual is an Officer in respect of the same contravention; and
- the contravention took place with the Officer's consent or connivance or was attributable to any neglect on the part of the Officer.

Why do we issue MPNs against Officers?

When appropriate, we issue MPNs against Officers to act as a further deterrent and to ensure future compliance with PECR. This is particularly true in circumstances when we would not fully achieve that effect by only issuing an MPN against the Body.

When would it be appropriate to issue an MPN against an Officer?

In addition to the statutory requirements above, we consider it appropriate to serve an MPN on an Officer in various circumstances, including (but not limited to) situations where:

- the Body goes into liquidation or took measures to avoid paying an MPN;
- the Body has no or limited ability to pay an MPN, but the Officer does have the ability to pay;
- the Officer is or was an Officer of another Body which received an MPN for a contravention of PECR;
- the Officer or the Body has a history of PECR contraventions; or
- serving an MPN on the Officer would deter future contraventions of, and promote compliance with, PECR.

Calculation of the penalties

How do we calculate the level of penalties?

Once we decide to impose an MPN, we must then consider what amount is appropriate, given the individual circumstances of each case.

In determining the amount, we consider the aims of why we issue MPNs, and the general factors detailed above which we consider when deciding whether to issue an MPN.

We may also take into consideration additional factors where relevant, such as:

- the type of people affected (for example, vulnerable adults);
- whether the contravention was a 'one-off' or part of a series of similar contraventions;
- whether circumstances outside of the direct control of the person, organisation or Officer caused or exacerbated the contravention, for example, if a data processor or an employee acted inappropriately;
- what steps, if any, the person, organisation or Officer took once they became aware of the contravention (for example concealing it, voluntarily reporting it to us or not taking action once we or another body identified the contravention);
- the role of senior managers, who we would expect to demonstrate higher standards of behaviour;
- whether there was any lack of co-operation or deliberate frustration, eg failure to respond to our reasonable requests for information during the course of the investigation; or
- whether the person, organisation or Officer expressly, and without reasonable cause, refused to submit to a voluntary assessment or audit which could reasonably have revealed a risk of the contravention.

This list is not exhaustive.

How do we consider the financial impact on the person, organisation or Officer?

We aim to eliminate any financial gain or benefit the person, organisation or Officer obtains from non-compliance with PECR.

We take into account the sector, for example whether the person, organisation or Officer concerned is involved in the voluntary sector. We also consider the person, organisation or Officer's size, and financial or other resources.

We consider whether liability to pay the fine falls on the public and, if so, their status (for example, charitable trustees in the voluntary sector).

We consider the likely impact of the penalty on the person, organisation or Officer concerned, in particular financial and reputational impact.

We take into account any proof of genuine financial hardship which they provide to us. The purpose of an MPN is not to impose undue financial hardship on an otherwise responsible person, organisation or Officer.

We consider agreeing payment of MPNs in instalments. This would depend on the recipient showing, to our satisfaction, that there are economic, financial or other reasons, why this is necessary.

We would not make any agreement to allow payment in instalments where the payment would no longer be effective and dissuasive.

What other considerations do we take into account?

If we consider that a precedent or point of principle is relevant to a decision in a particular case, we would explain that relevance.

If we consider there are other factors, not referred to above, that are relevant in a particular case to the determination of the MPN's amount, we would explain what these are.

Having considered the relevant factors in relation to the particular facts and circumstances of the contravention under consideration, we then determine the level of an MPN.

Regulation 2 of the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010/31, states that the amount of an MPN served must not exceed £500,000.

What is the process?

If we believe it may be necessary to issue an MPN, we first issue a Notice of Intent (NoI). The NoI explains why we believe a monetary penalty notice is necessary and sets out details of the proposed penalty.

The NoI sets out the proposed MPN amount and informs the recipient that they may make written representations in relation to the proposed MPN within a specified period. The NoI also contains such other information as is prescribed in the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010.

An NoI must contain:

- the name and address of the person, organisation or Officer;
- the grounds on which we propose to serve an MPN, including:

    - the nature of the personal data involved in the contravention;
    - a description of the circumstances of the contravention;
    - the reason we consider that the contravention is serious;
    - whether we consider that section 55A(2) or section 55A(3) applies, and the reason we take this view;
- an indication of the amount of the MPN we propose to impose and any aggravating or mitigating features we took into account; and
- the date on which we propose to serve the MPN.

The NoI must specify a period within which the recipient can make written representations to us. This period must be reasonable and must not be less than 21 days, beginning with the first day after serving the NoI.

What if a recipient does not agree with the content of an NOI?

The NoI's purpose is to set out the proposed MPN and enable the recipient to make representations to us. The recipient may wish to:

- comment on the facts and views set out in the NoI;
- make general remarks on the case; or
- enclose documents or other material such as financial details.

The NoI's recipient should also inform us if we need to redact any confidential or commercially sensitive information from an MPN.

We must consider any written representations made in relation to an NoI when deciding whether to serve an MPN. Following expiry of the period referred to above, we will take the following steps and:

- reconsider the amount of the MPN generally, and whether it is a reasonable and proportionate means of achieving the objective or objectives which we seek to achieve by this imposition;
- ensure that the monetary penalty is within the prescribed limit of £500,000; and
- ensure that we are not, by imposing an MPN, acting inconsistently with any of our statutory duties and that an MPN would not impose undue financial hardship on an otherwise responsible Person.

Having taken full account of any representations and any other circumstances relevant to the particular case under consideration, we then decide whether or not to impose an MPN and, if so, determine an appropriate and proportionate amount.

The MPN should not be substantially different to the amount proposed in the NoI, unless the representations of the person, organisation or Officer can justify a reduction.

We must either serve an MPN or write to the person, organisation or Officer advising that we are not taking further action in regard to the contravention specified in the NoI. We may not serve an MPN if a period of six months elapses after the service of the NoI.

What would an MPN contain?

We may serve an MPN on a person, organisation or Officer requiring them to pay a monetary penalty of an amount we determine and that the MPN specifies.

The MPN must contain such information as is prescribed in the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010.

An MPN must contain:

- the name and address of the person, organisation or Officer;
- details of the served NoI;
- whether we received written representations following the service of the NoI;
- the grounds on which we impose the MPN, including:
    - the nature of the personal data involved in the contravention;
    - a description of the circumstances of the contravention;
    - the reason the Commissioner is satisfied that the contravention is serious;
    - in respect of a contravention of the Act, the reason the ICO is satisfied that the contravention is of a kind likely to cause substantial damage or substantial distress; and
    - whether the ICO is satisfied that section 55A(2) applies, or that section 55A(3) applies, and the reason the Commissioner is so satisfied;
- the reasons for the amount of the monetary penalty including any aggravating or mitigating features the Commissioner took into account when setting the amount;
- details of how the monetary penalty is to be paid;
- details of, including the time limit for, the right of appeal of the officer or body against:
    - the imposition of the monetary penalty, and
    - the amount of the monetary penalty; and
- details of our enforcement powers under section 55D.

We would publish the MPN on our website with any confidential or commercially sensitive information redacted.

Early payment reduction

We would reduce the monetary penalty by 20% if we receive full payment within 28 calendar days of sending the MPN. This early payment reduction does not apply in circumstances where we agreed an instalment plan.

Applications for variation of an MPN

We may serve a variation notice (a notice that we propose to vary an MPN). The notice:

- identifies the notice concerned;
- specifies how the notice is to be varied; and
- specifies the date on which the variation is to take effect.

We would publish any notice of variation of the MPN on our website with any confidential or commercially sensitive information redacted.

The variation notice extends 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 an MPN

We may not take action to enforce a monetary penalty unless:

- the period specified in the MPN within which a monetary penalty is due expires and all or any of the monetary penalty has not been paid;
- all relevant appeals against the MPN and any variation of it have either been decided or withdrawn; and
- the period to appeal against the monetary penalty and any variation of it has expired.

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.

Applications for cancellation of an MPN

We can cancel an MPN by serving a cancellation notice. A cancellation notice is a notice that an MPN ceases to have effect. A cancellation notice:

- identifies the notice concerned;
- states that we are cancelling the notice concerned; and
- states the reasons for the cancellation.

We publish any notice of cancellation of the MPN on our website with any confidential or commercially sensitive information redacted.

Right of appeal

Recipients of an MPN or variation notice may appeal to the First-tier Tribunal against a variation notice or the issue of the MPN and the amount specified in the MPN, or both. Each MPN specifies the period within which the recipient must either pay the monetary penalty or make an appeal. For the appeals procedure, please refer to The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules.

Further reading

The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 (legislation.gov.uk)

The Data Protection (Monetary Penalties) Order 2010

General Regulatory Chamber tribunal procedure rules - GOV.UK (www.gov.uk)

Evaluation and next steps

We will keep this guidance under review and will update it, as and when necessary, to reflect any amendments to the legislation which this guidance covers.