

New powers for the Information Commissioner

From 6 April 2010 the Information Commissioner (the Commissioner) will have the power to issue a monetary penalty notice (MPN) against your business if it has committed a serious data protection breach.

What is an MPN?

An MPN is a notice requiring a data controller to pay a fine set by the Commissioner. The amount of the MPN determined by the Commissioner must not exceed **£500,000**.

Who is a data controller?

A data controller is the person (or business) who decides the purposes for which, and the manner in which, any personal data is processed.

When can an MPN be issued?

In order to issue an MPN the Commissioner must be satisfied that:

- The data controller has **seriously contravened** the data protection principles; and
- The contravention was likely to cause **substantial damage** or **distress**, and either
 - The contravention was **deliberate**; or,
 - The data controller **knew or ought to have known** that there was a risk that the contravention would occur, and that it would be likely to cause substantial damage or distress, but still failed to take reasonable steps to prevent it from happening.

Before issuing the MPN the Commissioner must serve a **notice of intent** on the data controller, stating the intention to impose a fine and providing a set length of time to respond. The data controller can contest the issue of the MPN and/or the proposed size of the fine. The Commissioner must consider any representations and then decide whether to proceed with the imposition of the MPN. This is less likely where the data controller can show that reasonable preventative steps were taken.

A data controller can appeal to the Tribunals Services against the imposition of an MPN.

Serious contravention

A single breach may be sufficient to meet the threshold of a “serious contravention”. For example:

- Medical records containing sensitive personal data are lost during an office move.

What is meant by the term “substantial”?

The likelihood of damage or distress suffered by an individual will have to be considerable in importance, value, degree, amount or extent. For example:

- Inaccurate personal data held by an ex-employer is disclosed in an employment reference, resulting in the loss of a job opportunity for an individual.

What is meant by the term “damage”?

Damage is any financial loss suffered by an individual, such as loss of earnings. For example:

- Financial data is lost and an individual becomes the victim of identity fraud.

What is meant by the term “distress”?

Distress could be an injury to feelings or any anxiety suffered by an individual. For example:

- Medical details are stolen and an individual suffers worry and anxiety that their sensitive personal data will be made public, even if it does not actually happen.

What is meant by the term “deliberate” contravention?

The contravention is deliberate or premeditated. For example:

- A marketing company collects personal data for the purposes of a competition. It then uses the same data for other commercial purposes without informing the individuals concerned.

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

A data controller is aware or should be aware of a risk that a contravention will occur. For example:

- A data controller is warned by its IT department that employees are accessing sensitive personal data but fails to carry out a risk assessment or implement a policy of encrypting all laptops and removable media as appropriate.

What factors will determine the amount of the MPN?

A number of factors will be taken into consideration before deciding the level that the MPN will be set at, including:

- Whether the contravention was a “one-off” or part of a series of similar breaches.
- Whether there was a deliberate lack of co-operation (for example, a failure to respond to reasonable requests for information during the investigation).
- What steps were taken once the data controller became aware of the breach (for example, concealing it or voluntarily reporting the contravention).

What steps can a business take to avoid the imposition of an MPN or notice of intent?

- Ensure that you can provide evidence that your business has recognised the risks of handling personal data and has taken action to address the issue (for example, you have conducted a risk assessment).
- Put in place appropriate policies, practices and procedures to avoid potential data protection breaches within your business (for example, by establishing a robust compliance regime).
- Pay particular attention to data protection issues where personal data of large numbers of individuals or sensitive data is concerned.
- Implement any guidance or codes of practice published by the Commissioner or other regulatory bodies that may be relevant to potential data protection breaches within your business.
- Do not allow any known issues to remain unresolved (for example, rectify any problems with your IT systems as soon as possible).