Administrative Data Research Network

An ESRC Data Investment

Penalties for serious breaches of the Data Protection Act (Monetary Penalty Notices)

Introduction

This is a guide to the legal sanctions which already exist to prevent data breaches. In addition to these, any researcher not following Administrative Data Research Network guidelines would also face serious sanctions from data custodians, Research Councils UK (RCUK) and funders. These include stiff penalties both for them and the institution they work for, which would significantly damage their future career in research.

Legal penalties

The Information Commissioner may order data controllers to pay penalties up to £500,000 for serious breaches of the data protection principles contained in the Data Protection Act (DPA) dating from or after 6 April 2010. The monetary penalty notices will only apply to serious contraventions of the DPA occurring on or after 6 April 2010 by all data controllers in the UK, whether in the private, public or voluntary sectors (except for Crown Estate Commissioners or persons specified by s.63(3) DPA).

The Information Commissioner's Office (ICO) has produced statutory guidance about how it proposes to use this new power.

A monetary penalty notice can only be imposed on a data controller. A monetary penalty notice cannot be imposed on a data processor, where processing of personal data is carried out on behalf of a data controller, or against an individual processing personal data for domestic use.

A data controller is the entity responsible for complying with data protection law, which in most cases will be a company or authority, rather than an individual. Section 1(1) of the Data Protection Act defines a data controller as 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any data are, or are to be, processed'.

The way in which a researcher handles personal data will determine whether or not a researcher becomes a data controller, and consequently whether or not a monetary penalty notice could be prepared and issued against that individual. A researcher may become a data controller in his/her own right where data is used for that individual's own purposes, and he/she may therefore be liable to be served with a monetary penalty notice if any of the data protection principles are breached. More information on data protection principles

Example

Where a researcher has been provided with personal data for research purposes from a data holding organisation, and that researcher then passes the data onto a third party who uses the data for purposes other than it was originally obtained for, either the researcher or the data holding organisation could be liable to be served with a monetary penalty notice for any serious breach of the data protection principles, depending on the surrounding circumstances. If the data holding organisation had simply provided the data to the researcher, without ensuring that the data would only be used for the specified and lawful purpose for which it was obtained, and that it was going to be kept securely etc., and the researcher then used it for some unlawful purpose, the data holding organisation could be in breach of one of the data protection principles (for example, relating to security) and consequently be liable for a monetary penalty. However, if the data holding organisation acts entirely properly and ensures that it has complied with all the data protection principles, but it is the researcher who nevertheless uses the data improperly, then the researcher could be liable for any breach, and consequently a monetary penalty notice could be issued against that individual.

It is therefore possible that a researcher can in certain circumstances become a data controller, and where there is a serious breach of the DPA data protection principles, the researcher could consequently become liable for a monetary penalty. However, it is more likely that a researcher will have a relationship with a data controller (an organisation such as a University or research institute) which is responsible for compliance with data protection issues.

Data controllers are obliged to comply with data protection legislation, and they are liable for any breaches of data protection law which are caused by their own actions or by those of their data processors. Monetary penalties would not usually apply to individual researchers where the data holding organisation is liable for breach of a data protection principle, unless the organisation has applied the data protection principles, and it is the researcher who acts in breach of his/her contract and breaches a data protection principle (see the example above).

ICO Guidance

Under s.55A and s.55B of the Data Protection Act, the Information Commissioner may in certain serious circumstances of contravention of the data protection principles serve a monetary penalty notice on a data controller to pay a penalty not exceeding £500,000.

A monetary penalty notice may be imposed if a data controller has seriously contravened the data protection principles, and the Information Commissioner is satisfied that

a. there has been a serious contravention of section 4(4) of the Act by the data controller
   [i.e. failure by the data controller to comply with one of the data protection principles, such as a failure to take adequate security measures]

and

b. the contravention was of a kind likely to cause substantial damage or substantial distress
   [i.e. real, rather than merely perceived, damage which can be financially

quantified as a loss suffered by an individual; or which causes an individual substantial injury to feelings, harm or anxiety]

and either

c. the contravention was deliberate
[e.g. collecting personal data for one purpose, then using it for another without consent or informing the individual concerned]

or

d. the data controller knew or ought to have known [i.e. been aware] 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
[e.g. carry out a risk assessment or have good governance in place for preventing data protection contraventions; reasonable steps are to be assessed on a case by case basis].

As a starting point the ICO 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 data protection principles by a data controller and that the other statutory requirements apply. The framework in appendix A is used to help determine this.

The standard of care to be applied by a data controller is that of a reasonably prudent data controller. The objective in imposing a monetary penalty notice is to encourage compliance with the DPA, or at least to act as a deterrent against non-compliance. The penalties are therefore designed to act both as a sanction and as a deterrent to non-compliance, so as to promote compliance with the DPA.

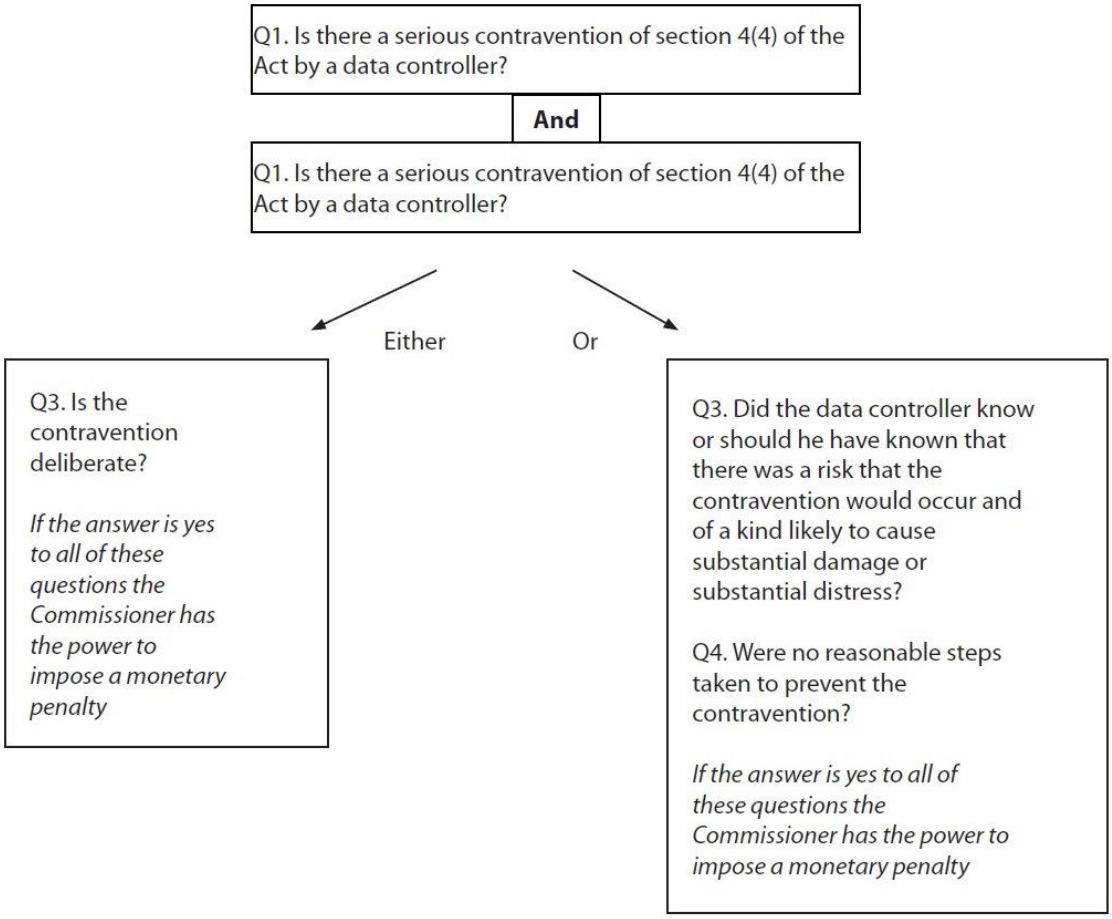
Essentially the power conferred upon the Information Commissioner will therefore be used as a sanction against a data controller who deliberately or negligently disregards the law. The Commissioner will take a proportionate and objective approach in considering whether the contravention has been serious, aiming to reflect the reasonable expectations of individuals and society and ensure that any harm is genuine and capable of explanation. A single serious breach of a data protection principle may be sufficient to meet this threshold.

The Information Commissioner must initially serve a notice of intent on a data controller if he proposes to serve a monetary penalty notice, setting out the proposed amount of the monetary penalty. The Commissioner must consider the appropriate amount of the penalty, taking into account such factors as the seriousness of the data contravention, the effect of the contravention, the sector, size, financial and other resources of a data controller. The monetary penalty will be reasonable and proportionate to the seriousness of the breach.

A data controller can respond to the notice of intent, and any written representations must be considered by the Commissioner when deciding whether to serve a monetary penalty notice. A data controller on whom a monetary penalty notice is served may appeal against it.

In addition to the new power for the Information Commissioner to issue monetary penalty notices, the Commissioner may still serve an Enforcement Notice under s.40 of the DPA where he is satisfied that a data controller has contravened any of the data protection principles, which requires a data controller to take, or refrain from taking certain steps, or to refrain from processing any personal data.

Data Protection Act serious contravention framework



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

Please note that any advice provided by the Administrative Data Research Network is for information only and not legal advice. If you are unsure about any aspect of administrative data research, please consult your legal department or the relevant data holding organisation.