Data Protection Act 1998

Monetary Penalty Notice

Dated: 28 February 2014

Name: British Pregnancy Advice Service

Address: 20, Timothy's Bridge Road, Stratford Enterprise Park, Stratford on Avon CV37 9BF

Statutory framework

---

1. The British Pregnancy Advice Service ('BPAS') is a registered charity and is also the data controller, as defined in section 1(1) of the Data Protection Act 1998 (the "Act"), in respect of the processing of personal data carried out by BPAS. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which he is the data controller.

2. The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act"). By virtue of section 6(1) of the Act, the office of the Data Protection Registrar originally established by section 3(1)(a) of the 1984 Act became known as the Data Protection Commissioner. From 30 January 2001, by virtue of section 18(1) of the Freedom of Information Act 2000 the Data Protection Commissioner became known instead as the Information Commissioner (the "Commissioner").

3. Under sections 55A and 55B of the Act (introduced by the Criminal Justice and Immigration Act 2008 which came into force on 6 April 2010) the Commissioner may, in certain circumstances, where there has there been a serious contravention of section 4(4) of the Act, serve a monetary penalty notice on a data controller requiring the data controller to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice but not exceeding £500,000. The Commissioner has issued Statutory Guidance under section 55C (1) of the Act about the issuing of monetary penalties which is published on the Commissioner's website. 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.

Power of Commissioner to impose a monetary penalty

(1) Under section 55A of the Act the Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that –

(a) there has been a serious contravention of section 4(4) of the Act by the data controller,

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

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller –

(a) knew or ought to have known –

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

Background

1. On 8 March 2012, an attacker used an automated tool to identify website vulnerabilities in an attempt to gain unauthorised access to the BPAS website content management system ('CMS'). Such tools are widely available on the internet and target well known vulnerabilities and poor website coding practices. BPAS were alerted to the incident by staff when it was noticed that the BPAS website had been defaced by the attacker.

2. The BPAS website enabled users to request a call back for advice. To access the call back service, users had to use a web form to submit their contact details to BPAS. The website then retained a copy of the

call back details of approximately 9,900 individuals unnecessarily and this information was available to the attacker once he gained access to the CMS. The call back details consisted of the user's name, date of birth, address and telephone number (the 'call back details'). However, patient medical records were hosted entirely separately by BPAS and not available to the attacker.

3. A statement on the BPAS website clearly described the services on offer at BPAS such as contraceptive advice, abortion, counselling, STI screening, sterilisation, vasectomy and treatment for erectile dysfunction. Therefore, the individuals who submitted their details for a call back were more than likely to require advice in relation to one or more of these services provided by BPAS.

4. BPAS reported the website attack to the police on 9 March 2012 and the attacker was arrested on 10 March 2012. The police had to react quickly due to the context of the information that was accessed and the risks associated with the attack. Some of the call back details were from individuals whose ethnicity and social background could have led to physical harm or even death if the information had been disclosed by the attacker.

5. The attacker targeted the BPAS website because he disagreed with abortion and wanted to cause trouble for the organisation which is the largest provider of abortion services in the UK. He did not expect to gain access to the call back details but having done so, the attacker publicly expressed his intention to publish the names of the individuals whose call back details were held on the BPAS website. Fortunately, the attacker did not publish this information which was recovered by the police following an injunction obtained by BPAS.

6. In 2007, an IT company was instructed to develop the BPAS website which was initially designed to have an online 'appointment booking service' so that users could book an appointment to receive a call back. Subsequently, BPAS decided against this feature mainly due to concerns over the security of the data. In the absence of any further specification, BPAS mistakenly assumed that the scaled down CMS function would only generate an email when users completed the 'call back web form' which would be sent to the secure email server with no call back data being retained on the website.

7. In 2008 (due to concerns about the IT company's performance) BPAS decided to instruct another IT company to host the BPAS website. BPAS was not aware that it was processing the call back data, and as a consequence BPAS did not ensure that administrative passwords were stored securely or that stated standards of communication

confidentiality were met. BPAS also failed to carry out appropriate security testing on the website which would have alerted them to the vulnerabilities that were present and did not ensure that the underlying software supporting the website was kept up to date. BPAS did not have a written contract with either company that complied with the requirements of the Act.

8. The Commissioner understands that BPAS have now removed the call back details from the website and taken substantial remedial action to ensure that this security breach will not be repeated.

Grounds on which the Commissioner proposes to serve a monetary penalty notice

---

The relevant provision of the Act is the Seventh Data Protection Principle which provides, at Part I of Schedule 1 to the Act, that:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

Paragraph 9 at Part II of Schedule 1 to the Act provides that:

"Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to -

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected".

Paragraph 11 at Part II of Schedule 1 to the Act provides that:

"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle-

(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

(b) take reasonable steps to ensure compliance with those measures.

Paragraph 12 at Part II of Schedule 1 to the Act further provides that:

"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless-

(a) the processing is carried out under a contract-

(i) which is made or evidenced in writing, and

(ii) under which the data processor is to act only on instructions from the data controller, and

(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

In deciding to issue this Monetary Penalty Notice, the Commissioner has considered the facts of the case and the deliberations of those within his office who have recommended this course of action. In particular, he has considered whether the criteria for the imposition of a monetary penalty have been met; whether, given the particular circumstances of this case and the underlying objective in imposing a monetary penalty, the imposition of such a penalty is justified and whether the amount of the proposed penalty is proportionate.

- The Commissioner is satisfied that there has been a serious contravention of the Seventh Data Protection Principle.

  In particular, BPAS failed to take appropriate technical and organisational measures against the unauthorised processing of personal data stored on the BPAS website such as having a detailed specification about the parameters of the CMS to ensure that either the website did not store any personal data or alternatively, that effective and appropriate security measures were applied such as storing administrative passwords securely; ensuring stated standards of communication confidentiality were met; carrying out appropriate security testing on the website which would have alerted them to the vulnerabilities that were present or ensuring that the underlying software supporting the website was kept up to date.

  The Commissioner considers that the contravention is serious because BPAS were unaware that personal data was held on the website in such a way that the call back details of 9,900 users were unprotected from an attack of this type. This is unacceptable in view of the nature of the information held on the website which was held in the context of the extremely personal and sensitive services provided by BPAS and which

should have been afforded the highest standards of security.

In the circumstances, BPAS should also have complied with the requirements set out in paragraphs 11 and 12 in Part II of Schedule 1 to the Act.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial damage or substantial distress. Confidential personal data was at risk of unauthorised processing due to the inappropriate technical and organisational measures taken by BPAS.

  The privacy policy on the BPAS website led its users to believe that every effort had been made to keep their information secure and that the call back details would remain confidential and accessible to only those who need to know that information. BPAS failed in this regard by failing to provide an encrypted communication protocol between user and web server.

  The failure to take appropriate technical and organisational measures was likely to cause substantial distress to the users of the website even if this is simply by knowing that their confidential personal data has in fact been accessed by the attacker (despite the assurance given by BPAS) who had no right to see that information.

  Further, the users of the BPAS website would be likely to be distressed by justifiable concerns that their data may be further disseminated even if those concerns do not actually materialise.

  Fortunately, given the motivation of the attacker, an injunction was obtained by BPAS and the call back details were recovered by the police before the attacker contacted the media or otherwise sought to exploit the information for his own ends. This confirms that the contravention was of a kind likely to cause substantial distress even if it can be argued that substantial distress was not actually caused in this case.

  It is also noted that BPAS decided not to inform the affected individuals following this security breach so as not to cause further distress.

  If the data was to be misused by those who had access to it or if it was in fact disclosed to other untrustworthy third parties then it is likely that the contravention would cause further distress and also substantial damage to the users of the website such as physical harm or even death in extremis.

- The Commissioner is satisfied that section 55A (3) of the Act applies in that 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.

  The Commissioner has taken this view because of the nature of the personal data held on the website in the context of the extremely personal and sensitive services provided by BPAS. Although BPAS was unaware that the call back details were held on the website they knew that the call back details had to be held securely which is why they moved away from an 'appointment booking system' and provided assurances about security in their privacy policy.

  In the circumstances, the data controller knew or ought to have known that there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention such as having a detailed specification about the parameters of the CMS to ensure that either the website did not store any personal data or alternatively, that effective and appropriate security measures were applied such as storing administrative passwords securely; ensuring that stated standards of communication confidentiality were met; carrying out appropriate security testing on the website which would have alerted them to the vulnerabilities that were present or ensuring that the underlying software supporting the website was kept up to date.

  Further, it should have been obvious to BPAS because of the nature of the personal data held on the website which was held in the context of the extremely personal and sensitive services provided by BPAS that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the users of the website.

Aggravating features the Commissioner has taken into account in determining the amount of a monetary penalty

---

Impact on the data controller

- Sufficient financial resources to pay a monetary penalty up to the maximum without causing undue financial hardship

Mitigating features the Commissioner has taken into account in determining the amount of the monetary penalty

Nature of the contravention

- BPAS website was attacked by an individual who was convicted of criminal offences under the Computer Misuse Act 1990

Effect of the contravention

- BPAS obtained an injunction to prevent publication of the call back details within 12 hours of the attack
- As far as the Commissioner is aware the call back details have not been further disseminated

Behavioural issues

- Voluntarily reported to Commissioner's office
- BPAS have been fully co-operative with the Commissioner's office
- Substantial remedial action has now been taken

Impact on the data controller

- BPAS is a registered charity and undertakes charitable work as well as providing services on behalf of the NHS
- Significant impact on BPAS's reputation as a result of this security breach
- Security breach was publicised in the media

Other considerations

- The Fifth Data Protection Principle at Part I of Schedule 1 to the Act was also contravened by BPAS in that the call back details were kept for five years longer than was necessary for its purposes
- The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to personal data stored on their websites

Notice of Intent

A notice of intent was served on the data controller dated 16 December 2013. The Commissioner received written representations from the data controller's Chief Executive dated 8 February 2014 in response to the notice of intent. In the circumstances, the Commissioner has now taken the following steps:

- reconsidered the amount of the monetary penalty generally, and whether it is a reasonable and proportionate means of achieving the objective which the Commissioner seeks to achieve by this imposition;
- ensured that the monetary penalty is within the prescribed limit of £500,000; and
- ensured that the Commissioner is not, by imposing a monetary penalty, acting inconsistently with any of his statutory or public law duties and that a monetary penalty notice will not impose undue financial hardship on an otherwise responsible data controller.

Amount of the monetary penalty

The Commissioner considers that the contravention of the seventh data protection principle is "very serious" and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of **£200,000** (Two hundred thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

In reaching this decision, the Commissioner considered other cases of a similar nature in which a monetary penalty had been imposed, and the facts and aggravating and mitigating features referred to above. Of particular relevance is the fact that 9,900 individuals entrusted their call back details to BPAS and they were then exposed to the risk of significant harm due to serious failings by BPAS.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 1 April 2014 at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

Early payment discount

If the Commissioner receives full payment of the monetary penalty by 31 March 2014 the Commissioner will reduce the monetary penalty by 20% to **£160,000** (One hundred and sixty thousand pounds). You should be aware that if you decide to take advantage of the early payment discount you will forfeit your right of appeal.

Right of Appeal

There is a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against:

a. the imposition of the monetary penalty

and/or;

b. the amount of the penalty specified in the monetary penalty notice.

Any Notice of Appeal should be served on the Tribunal by 5pm on 31 March 2014 at the latest. If the notice of appeal is served late the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

Information about appeals is set out in the attached Annex 1.

Enforcement

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

- the period specified in the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;
- all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and
- the period for the data controller to appeal against the monetary penalty and any variation of it has expired.

In England, Wales and Northern Ireland, the monetary penalty is

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

Dated the 28th day of February 2014

Signed: ……

David Smith
Deputy Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation notice has been served a right of appeal to the (First-tier Tribunal) General Regulatory Chamber (the "Tribunal") against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Arnhem House
   31 Waterloo Way
   Leicester
   LE1 8DJ

   a) The notice of appeal should be served on the Tribunal by 5pm on 31 March 2014 at the latest.

   b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

d) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

e) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).