Data Protection Act 1998

Monetary Penalty Notice

Dated: 14 January 2013

Name: Sony Computer Entertainment Europe Limited

Address: 10, Great Marlborough Street, London W1F 7LP

Statutory framework

1. Sony Computer Entertainment Europe Limited ("SCEE") is 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 SCEE and is referred to in this notice as the "data controller". 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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

4. Sony Network Entertainment Europe Limited ("SNEE") (a wholly owned subsidiary of SCEE) operates a "PlayStation" Network Platform (the "Network Platform") in a territory which covers Europe, the Middle East, Africa, Australia and New Zealand. SCEE is the data controller in respect of the personal data provided by customers when they create an account to access the Network Platform. The Network Platform, including the Playstation customer databases, was administered and maintained on the data controller's behalf by a US service provider (which is part of the Sony group). The Network Platform was used by

an estimated [redacted] million customers in Europe, the Middle East, Africa, Australia and New Zealand with [redacted] million of those customers based in the UK.

5. [redacted], the Network Platform was infiltrated following several Distributed Denial of Service (DDoS) attacks on various online networks of the Sony group. The attacker accessed personal data stored on the Network Platform which included customers' names; addresses; email addresses; dates of birth and account passwords. These same details, including passwords, will have, in at least some cases, been used by customers and data controllers to control the customer's access to other online and offline services.

6. The Commissioner is aware that the data controller made some efforts to protect account passwords. However the data controller failed to ensure that the Network Platform service provider kept up with technical developments. Therefore the means used would not, at the time of the attack, be deemed appropriate, given the technical resources available to the data controller.

7. [redacted]

8. In addition, it is estimated that [redacted] million of the customers had registered payment card details to their account although there is no evidence that the encrypted payment card details were accessed. [redacted] and the Network Platform team did not detect any unauthorised activity until 19 April 2011.

9. It is likely that the attacker gained access to the Network Platform through a vulnerability [redacted]

[redacted] However, the data controller failed to take the action required [redacted] to address the vulnerability even though appropriate updates were available. [redacted]

10. The Network Platform has now been completely rebuilt, including up to date and more sophisticated security measures. In particular, the Network Platform customer account passwords have been changed and appropriately protected; [redacted] and the software has been reconfigured to prevent any further exploitation.

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".

- The Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act.

  In particular, the data controller failed to ensure that appropriate technical measures were taken against unauthorised or unlawful processing of personal data stored on the Network Platform such as additional cryptographic controls to protect passwords; [redacted] prior to the hacking attack and addressing the system vulnerabilities at the relevant time.

  The contravention is serious because the measures taken by the data controller did not ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing and the nature of the data to be protected.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial damage or substantial distress. The data controller's failure to ensure that appropriate technical measures were taken was likely to cause substantial damage or substantial distress to data subjects whose personal data has been or may have been accessed by third parties and could be further disclosed.

  In this particular case the data subjects have suffered from substantial distress knowing that their personal data has been or may have been accessed by third parties and could have been further disclosed even though, as far as the Commissioner is aware, this latter concern has not so far materialised.

  If the data was to be misused by those who have had access to it or is 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 data subjects such as exposing them to possible fraud.

- 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.

  Various online networks of the Sony group had been subjected to several DDoS attacks prior to the attack on [redacted]. Therefore, the data controller should have anticipated a further attack on its systems and taken appropriate security measures.

Instead, the data controller was storing vast amounts of personal data (including financial information and [redacted]) on the Network Platform at a time when the systems concerned were [redacted]

[redacted]

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 additional cryptographic controls to protect passwords; [redacted] prior to the hacking attack and addressing the system vulnerabilities at the relevant time.

Further, it should have been obvious to the data controller who was aware of the nature and amount of the personal data stored on the Network Platform that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the data subjects.

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

---

Nature of the contravention

- Contravention was particularly serious because of the nature and amount of personal data

Effect of the contravention

- Vast amount of personal data at risk relating to an estimated [redacted] million individuals
- Other online and offline accounts held by customers could have been placed at risk

Behavioural issues

- Data controller should have been aware of the software vulnerability [redacted]
- Network Platform service provider should have acted sooner
- Data controller is part of a multi national group of companies with sufficient resources to address security issues

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

- Data controller subject to a focused and determined criminal attack on the Network Platform even though it should have been anticipated
- The security breach occurred within a complex computer system
- Data controller had taken steps to secure some aspects of the Network Platform
- No previous similar security breach that the Commissioner is aware of

Effect of the contravention

- Personal data is unlikely to have been used for fraudulent purposes
- No complaints received to date

Behavioural issues

- Voluntarily reported to Commissioner's office
- Data subjects informed and reparation offered where appropriate, in the form of the "Welcome Back" package
- The data controller has been fully co-operative with the Commissioner's office
- Substantial remedial action has now been taken

Impact on the data controller

- [redacted]

- Significant impact on reputation of data controller as a result of this security breach

Other considerations

- The Third Data Protection Principle at Part I of Schedule 1 to the Act was also contravened in that excessive personal data [redacted] was stored on the Network Platform
- 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 computer systems

Notice of Intent

A notice of intent was served on the data controller dated 25 July 2012. The Commissioner received written representations from the Solicitor acting for the data controller dated 12 October 2012. The Commissioner has considered the written representations made in relation to the notice of intent when deciding whether to serve a monetary penalty notice. In particular, the Commissioner has 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 section 4(4) of the Act is very serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £250,000 (Two hundred and fifty thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 14 February 2013 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 13 February 2013 the Commissioner will reduce the monetary penalty by 20% to £200,000 (Two hundred thousand pounds).

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 13 February 2013 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 14th day of January 2013

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 13 February 2013 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)).