OnPoint Dechert LLP

January 2013 / Special Alert
A legal update from Dechert LLP

UK Data Protection Regulator ICO Flexes Power to Impose Fine

Sony Fined for Data Breach

Introduction

On 24 January 2013, the UK Information Commissioner's Office (ICO) served Sony Computer Entertainment Europe Limited ("Sony") with a monetary penalty of £250,000 following a serious breach of data security (the "Act").

The penalty comes following the well-publicised security breach which afflicted the Sony PlayStation Network Platform. This platform is the online element of Sony's PlayStation mobile gaming products and gaming console, allowing customers to chat and play against each other online as well as purchase games and rent films with credit cards. It was hacked in a targeted and concerted denial of service attack in 2011.

The UK's Power to Fine

The UK (in common with other EU member states) has implemented the European data protection directive as the cornerstone of its data protection law. A key element of that law is the requirement (principle 7 of the UK Data Protection Act 1998 or Article 17 of the EU directive 95/46) that all personal data is kept secure (the standard is using "appropriate technical and organisational measures") by the entity controlling that data. Until relatively recently, in the UK at least, transgression of this requirement would have been enforced by service of a notice requiring changes in the organisation (an "enforcement notice").

However, in April 2010, the UK regulator was given the power in limited circumstances to levy monetary penalties. The power arises where there has been a serious contravention of a data protection principle (such as the security principle). The ICO must be satisfied that there has been such a serious contravention, that the contravention was of a kind likely to cause substantial damage or substantial distress, and the data controller knew or ought to have known (a) that there was a risk that the contravention would occur; and (b) 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. If so, the ICO may serve a monetary penalty notice of an amount determined by the ICO up to a maximum of £500,000.

Whilst there have been some fines directed at the private sector, by and large most substantial fines to date have been against public bodies. One difficulty the regulator has in using these powers is to be satisfied that the threshold requirement that there has been "substantial damage" or "substantial distress" has been met. Another recent case, involving spam text messages sent to the general public, has demonstrated that the ICO takes a broad view as to what "substantial" means. It does not mean, according to this view, that each individual has to suffer substantial damage. Instead, the requirement is fulfilled if there are a substantial amount of individuals each suffering some (perhaps insubstantial) damage.

Sony's Breach

The Network Platform was hacked in April 2011 following several attacks on various online networks of the Sony Group. The attacker accessed personal information of millions of customers, including their names, addresses, email addresses, dates of birth and account passwords. Customers' payment card details were also put at risk, although there is no evidence that these were accessed. An ICO investigation found that Sony failed to ensure the Network Platform service provider kept up with technical developments and the attack could have been prevented the attack if the software had been up-to-date.

The Imposition of the Fine

The ICO found that Sony had breached the principle which states 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”.

The ICO was satisfied that there was a serious contravention of a relevant “data protection principle”, namely that Sony failed to ensure the appropriate technical measures were taken against unauthorised or unlawful processing of personal data. The measures taken by Sony did not ensure a level of security appropriate to the harm that might result from a breach. The notice served on Sony has been made public but with (for obvious security reasons) much of the details of the transgression redacted – although it is clear that the ICO considers that Sony had not kept up with the latest technological developments such as additional cryptographic controls to protect passwords.

The ICO was also satisfied that the breach was of a kind likely to cause substantial damage or substantial distress, in particular, the users of the Network Platform have suffered considerable distress knowing that their personal data has been or may have been accessed by third parties and could have been further disclosed.

The ICO ruled that Sony 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.

Taking into account some mitigating factors such as a voluntary notification of the breach and the substantial commercial damage to the Sony brand in this area, the fine imposed was £250,000 (reduced to £200,000 for prompt payment).

Two days after the fine was imposed, Sony announced that it would appeal the decision. The appeal is still pending.

Commentary

The fine is the third largest levied by the ICO, after a £325,000 penalty for Brighton and Sussex University Hospitals NHS Trust following the discovery of highly sensitive personal data belonging to thousands of patients and staff on hard drives sold on an internet auction site and a £300,000 fine imposed on the owner of Tetrus Telecoms, after that company sent millions of unlawful spam texts to the public. However, in the context of the size of Sony and the costs to Sony of the breach internationally (including damage to its brand) are estimated at $155.4 million this year], the size of the fine might be seen to be relatively modest.

It should be noted that the data protection rules in Europe are in the process of being revised. A new instrument (a directly enforceable data protection “Regulation”) was published in draft by the European Commission in 2012. Whilst still the subject of much inter-governmental negotiation, the initial draft contains significantly enhanced powers for regulators. All security and other data protection breaches would be subject to a fine, with no requirement to fulfil the threshold tests set out in the current UK regime such as “significant damage” or a requirement as to knowledge. Under this proposal, the maximum fine available to the ICO (in common with all European regulators) will be 2% of the annual global revenue of the entity that was responsible for the breach.

These proposals, together with proposed rules on data breach notification and other stringent requirements in the draft Regulation, will increasingly make European businesses (and multinationals with European operations) focus on proper compliance with data protection rules.

This update was authored by Renzo Marchini. If you have questions or for more information, please contact:

Timothy C. Blank
Boston
Send an email

Vernon L. Francis
Philadelphia
Send an email

Vivian A. Maese
New York
Send an email


T: +1 617 728 7154


T: +1 215 994 2577


T: +1 212 698 3520


Renzo Marchini
London
Send an email
T: +44 20 7184 7563


Joshua H. Rawson
New York
Send an email
T: +1 212 698 3862


Charles Wynn-Evans
London
Send an email
T: +44 20 7184 7545


To browse our library of legal updates, please visit dechert.com/publications

To see the full list of privacy and data protection lawyers, please visit our website.