

## **Civil Monetary Penalties – Setting the maximum penalty CP 48/09**

### **List of questions for response**

We would welcome responses to the following question set out in this consultation paper. Please email your completed form to: [victor.riega@justice.gsi.gov.uk](mailto:victor.riega@justice.gsi.gov.uk) or fax to: 020 3334 2245. Thank you.

**Question 1. Do you consider that a penalty of up to £500,000 provides the ICO with a proportionate sanction for serious contraventions of the data protection principles?**

Comments:

The National Association For Information Destruction – Europe (NAID-Europe) thanks the Ministry of Justice for the opportunity to comment on this issue. NAID-Europe is the European division of NAID, an international industry trade association of commercial data destruction service providers.

Our industry is closely involved with the practical implementation of data protection laws in many jurisdictions worldwide and, because improper data disposal is one of the most common ways in which the legal protection of personal data is (in practice) breached, NAID's input has often been sought by policy-makers seeking to address data protection issues.

We strongly support the creation and implementation of meaningful and substantial civil monetary penalties for serious contraventions of the data protection principles.

We consider that a penalty of up to £500,000 would provide ICO with a proportionate sanction for serious contraventions of the data protection principles, for the reasons described below.

We further submit that given the substantial financial resources of many larger data controllers, a maximum penalty of £500,000 is the lowest maximum penalty (of the three under consideration) that would offer ICO a meaningful sanction for serious contraventions of the data protection principles across the full range of all data protection controllers.

## **About NAID**

NAID has over 1,200 member locations, nearly 100 of which are in Europe and more than 20 of which are in the United Kingdom. NAID-Europe's headquarters are in Brussels, Belgium.

NAID's input has often been sought by policy makers seeking to address data protection issues. Our experience in the area of data protection is narrow and deep and as a result we have a unique perspective to offer on the issues.

In 2006, NAID received and accepted an invitation to be part of committee with the British Standards Institution (BSI) charged with creating operating practice standards for commercial enterprises offering secure destruction services. The end result, BS 8470, has now become a European Standard. NAID was also invited to provide an overview of the issue of data disposal to the Office of the Privacy Commissioner of Canada.

The U.S. Federal Trade Commission (FTC) sought NAID input during the rulemaking phase of implementing the Fair and Accurate Credit Transaction Act (FACTA) in 2003. FACTA was an amendment to the Fair Credit Reporting Act (FCRA), and introduced the first law specifically requiring the destruction of discarded information. (A law for which there is still no counterpart in Europe.)

NAID has also been invited to address the US Senate Financial Services Committee (in the hearings following the country's most notorious data breach involving Choicepoint in 2005), the committee within the Canadian House of Commons that was reviewing that country's national data protection law (the Personal Information Protection and Electronic Document Act (PIPEDA)) and similar committees in Alberta and British Columbia (in connection with their state privacy law reviews).

## **The Importance of Monetary Penalties to Regulatory Enforcement**

In 2003, the state of Georgia in the United States passed the first serious information destruction requirement. It contained strong enforcement language and had the support of the state's top law enforcement official, the state's Attorney General.

Soon after it became law, the NAID US headquarters received a phone call from an executive at a nationally known insurer. The caller asked for NAID Member locations in Georgia so he could arrange for destruction as required by the new law. When the NAID staff member mentioned that he could provide a list of members in all of the states, the caller, without hesitation, said that he did not need such a list outside of Georgia because

the other states didn't impose penalties for improper disposal.

NAID's experience is that this was an indicative rather than an unusual incident. It is clear that without the ability to apply monetary fines, regulatory enforcement can never achieve meaningful results. In particular organisations will not respond to data protection requirements unless there is sufficient impetus and consequences – positive or negative.

### **Data Protection Enforcement – A Case Study in the Effect of Penalties**

NAID's experience in the area of information disposal is that clear direction and meaningful fines used proportionately to penalise serious contraventions dramatically alter organisations' approach to and emphasis on proper information protection.

It is a well documented fact that improper disposal of personal information is a major cause of privacy breaches and identity theft. In our experience, the improper (insecure) disposal of information is rampant and in need of enforcement.

The epidemic of identity theft and the resulting problems it has caused in the United States is well known. Research shows that access to casually discarded personal information continues to be a leading source of the information needed for crime. As a result, in the United States, at both the state and federal level, there are laws requiring the destruction of personal information prior to disposal, having begun in 2003 in Georgia.

Although some organisations did change their disposal practices as a result of the mere implementation of the new laws, our observation was that most organisations did not take the regulations seriously until regulators began imposing fines for non-compliance over the last two years.

The first hint of a new enforcement regime regarding data disposal happened in December of 2007 when the US Federal Trade Commission (FTC) fined a small mortgage broker \$50,000.00 for improperly disposing of financial information under the Fair and Accurate Credit Transaction Act (FACTA) Final Disposal Rule. The incident received national attention, especially in the financial sector. We immediately saw a change in approach to proper disposal in that sector.

Enforcement has continued to increase and behaviour has changed for the better. Most recently, a hospital in Texas was fined \$990,000.00 for casually discarding several boxes of medical information in their outside disposal bin. In another recent enforcement action, CVS (the United States' largest retail pharmacy chain) was fined \$2,250,000.00 for casually

discarding medical information in violation of the Health Insurance Portability and Accountability Act (HIPAA).

Over the last two years, there have been approximately 15 such enforcement actions, with cumulative fines in the neighbourhood of \$10,000,000.00. The result has been a dramatic increase in attention to proper disposal methods.

The enforcement of information destruction requirements in the United States provides a unique opportunity observe the impact on how organisations on the role of enforcement in obtaining compliance with data protection requirements.

Prior to 2007, there was little if any enforcement of the destruction laws passed years earlier. Now regulators have begun to exercise their prerogative to enforce the laws and issue fines. There is no doubt that this change in tactics has begun to achieve the desired result.

#### **What Level of Penalty Achieves Results?**

It is clear that the maximum monetary penalty available to a regulator as an enforcement sanction is critical to the seriousness with which such sanction will be viewed both in absolute cost/benefit terms and in relation to likely publicity.

The proposed maximum figure of £500,000 for monetary penalties to be imposed by the Information Commissioner's Office (ICO) is certainly not excessive. We would argue that such a figure is highly unlikely to give rise to hardship in practice because it sets a maximum level of penalty, leaving the determination of an actual penalty as a matter with respect to which the ICO will have flexibility on a case-by-case basis. Any concerns in this area can be readily mitigated by the statutory guidance to be provided by the ICO; indeed the draft guidance published by the ICO addresses this point.

We note from the Ministry's Impact Assessment documentation that, within the European data protection regulatory community, a maximum penalty of £500,000 would be one of the highest available. However, It will be apparent from the examples given in the previous section that in the United States the penalties applied over the last two years have been comparable to that figure, and that fines of almost four times that sum have been imposed.

Within the wider international context, there is no scope to argue a maximum penalty of £500,000 would be disproportionate or out of step. The figure of £500,000 is in fact proportionate both to the sanctions available to equivalent regulators in other comparable jurisdictions and to the need to achieve deterrence in relation to larger data controllers (as

well as small and medium-sized entities).

### **Concluding Points**

Organisations need an impetus or consequences before they will change their behaviour regarding data protection. Without proportionate and meaningful financial penalties to assist enforcement the data protection principles will struggle for relevance and attention.

We strongly support imposing up to a £500,000 fine for serious contraventions of the data protection principles.

Again, we thank the Ministry of Justice for soliciting and considering comments and hope that ours may be of assistance in determining the further steps needed to improve compliance among data protection controllers with the data protection principles.

### **CONTACT INFORMATION**

NAID-Europe

Robert J. Johnson

Executive Director

287 Avenue Louise, 4th Fl.

1050 Brussels

Belgium

Telephone: +32 2 643 2045

Facsimile

Email: [info@naideurope.eu](mailto:info@naideurope.eu)

Website: [www.naideurope.eu](http://www.naideurope.eu)

## About you

Please use this section to tell us about yourself

<b>Full name</b>	ROBERT J JOHNSON
<b>Job title</b> or capacity in which you are responding to this consultation exercise (e.g. member of the public etc.)	EXECUTIVE DIRECTOR, NAID - EUROPE
<b>Date</b>	
<b>Company name/organisation</b> (if applicable):	NAID - EUROPE
<b>Address</b>	287 AVENUE LOUISE, 4TH FL., 1050 BRUSSELS, BELGIUM
<b>Postcode</b>	→
If you would like us to acknowledge receipt of your response, please tick this box	<input checked="" type="checkbox"/> (please tick box)
Address to which the acknowledgement should be sent, if different from above	ADDRESS ABOVE OR
	INFO@NAIDEUROPE.EU

If you are a representative of a group, please tell us the name of the group and give a summary of the people or organisations that you represent.

PLEASE SEE DETAILS PROVIDED IN COMMENT SUBMITTED (ATTACHED HERETO).

---



---



---