

Morrison & Foerster Client Alert

10 October 2013

ICO fine overturned: An eye off the ball but still on the money

By Amy Collins

For the first time ever, a fine issued by the UK Information Commissioner's Office ("ICO") has been overturned on appeal¹. On 21 August 2013, the UK Information Rights Tribunal ("Tribunal") handed down its preliminary decision overturning a £250,000 fine, which had been imposed by the ICO against the Scottish Borders Council ("SBC") for a data security breach². The Tribunal's decision raises the bar that needs to be met by the ICO in order to impose a fine for a breach of the Data Protection Act 1998 ("DPA"), emphasising that substantial damage or distress must be the *likely* result of the breach, and not a mere possibility.

BACKGROUND

On 10 September 2011, a member of the public noticed that a paper recycling bank in a supermarket car park had been overfilled with discarded files. The files contained various confidential personal data, including the name, address, national insurance number and date of birth of former employees and members of the SBC pension scheme and, in some cases, salary and bank account details.

The SBC had engaged a data processing company to transfer the information from 1,600 hard copy files to CDs, and to dispose of those hard copies, but had failed to put in place an appropriate data processing contract with sufficient guarantees in respect of the Seventh Data Protection Principle set out in the DPA.

ICO DECISION: AN EYE OFF THE BALL

The ICO can impose administrative fines of up to £500,000 in the event of a breach of a DPA Principle which is (a) serious, (b) of a kind likely to cause substantial damage or distress, and (c) either deliberate, or reckless and where no reasonable steps are taken to prevent it.

The ICO was satisfied that the breach was of a serious nature. It noted in particular that the SBC had failed to ensure that (i) appropriate technical and

UNITED STATES

California

Tiffany Cheung	(415) 268-6848
Rebekah Kaufman	(415) 268-6148
Christine E. Lyon	(650) 813-5770
David F. McDowell	(213) 892-5383
James R. McGuire	(415) 268-7013
Daniel F. Muto	(858) 720-7959
Purvi G. Patel	(213) 892-5296
Andrew Serwin	(858) 720-5134
William L. Stern	(415) 268-7637
Nancy R. Thomas	(213) 892-5561
David M. Walsh	(213) 892-5262

New York

Cindy Abramson	(212) 336-4178
Melissa Crespo	(212) 336-4354
John F. Delaney	(212) 468-8040
Sherman W. Kahn	(212) 468-8023
Mark P. Ladner	(212) 468-8035
Peter McLaughlin	(212) 336-4290
Michael B. Miller	(212) 468-8009
Suhna N. Pierce	(212) 336-4150
Marian Waldmann Agarwal	(212) 336-4230
Miriam H. Wugmeister	(212) 506-7213

Washington, D.C.

L. Richard Fischer	(202) 887-1566
D. Reed Freeman, Jr.	(202) 887-6948
Julie O'Neill	(202) 887-8764
Obrea O. Poindexter	(202) 887-8741
Cynthia J. Rich	(202) 778-1652
Andrew M. Smith	(202) 887-1558
Nathan David Taylor	(202) 778-1644

EUROPE

Brussels

Joanna Łopatowska	32 2 340 7365
Karin Retzer	32 2 340 7364
Alja Poler De Zwart	32 2 340 7360

London

Ann Bevitt	44 20 7920 4041
Anthony Nagle	44 20 7920 4029
Caroline Stakim	44 20 7920 4055
David Varney	44 20 7920 4058

ASIA

Beijing

Gabriel Bloch	86 10 5909 3367
Jingxiao Fang	86 10 5909 3382
Paul D. McKenzie	86 10 5909 3366

Hong Kong

Gordon A. Milner	852 2585 0808
------------------	---------------

Tokyo

Daniel P. Levison	81 3 3214 6717
Gabriel E. Meister	81 3 3214 6748
Jay Ponazacki	81 3 3214 6562
Toshihiro So	81 3 3214 6568
Yukihiro Terazawa	81 3 3214 6585

¹[http://www.informationtribunal.gov.uk/DBFiles/Decision/i1085/Scottish%20Borders%20Council%20EA.2012.0212%20\(26.09.13\)%20Final%20Decision.pdf](http://www.informationtribunal.gov.uk/DBFiles/Decision/i1085/Scottish%20Borders%20Council%20EA.2012.0212%20(26.09.13)%20Final%20Decision.pdf).

²[http://www.informationtribunal.gov.uk/DBFiles/Decision/i1068/Scottish%20Borders%20Council%20EA.2012.0212%20\(210813\)%20Preliminary%20Decision.pdf](http://www.informationtribunal.gov.uk/DBFiles/Decision/i1068/Scottish%20Borders%20Council%20EA.2012.0212%20(210813)%20Preliminary%20Decision.pdf).

Client Alert

organisational security measures governing the processing to be carried out were in place and (ii) the data processor would take reasonable steps to ensure compliance with those measures.

For example, the ICO stated that such security measures might have provided for the secure disposal of the files after scanning and stipulated that the data processor would either return the documents to the SBC in person, or securely destroy them and provide the SBC with a certificate of destruction. The ICO also commented that the SBC should have put in place regular monitoring to ensure compliance with these measures (because it became apparent during the ICO's investigation that the data processing company had been disposing of original documents in paper recycling banks for a period of up to seven years prior to the discovery of the breach).

The ICO was also satisfied that the breach was of a kind likely to cause substantial damage or distress to any data subject whose confidential personal data was seen by a member of the public. Data subjects, the ICO said, would be justifiably concerned that their data might be disseminated further, even if those concerns did not actually materialise. Further, if the data were disclosed to untrustworthy third parties, it was likely that further distress and substantial damage would be caused, including by exposing data subjects to the risk of identity fraud and financial loss.

In the ICO's view, the SBC knew or ought to have known of the risk of contravention, and failed to take reasonable steps to prevent it.

In light of its underlying objective to promote compliance with the DPA, and in order to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to hard copy personal data held in files, the ICO issued what it considered to be a reasonable and proportionate fine. In doing so, the ICO commented that the breach was a "*classic case of an organisation taking its eye off the ball when it came to outsourcing*".

TRIBUNAL DECISION: STILL ON THE MONEY

However, while the Tribunal agreed with the ICO's conclusion that there had been a breach of the DPA, and that that breach was serious, it did not consider that the breach was "*of a kind likely to cause substantial damage or substantial distress*". Consequently, the fine was not justified and the Tribunal ordered that the amount already paid to the ICO by the SBC should be returned.

The Tribunal emphasised that, in establishing the "likelihood" of substantial damage or distress, it was unnecessary for the ICO to establish that any harm had actually occurred or that the substantial damage or distress should "on the balance of probabilities" flow from the breach. The Tribunal referred to earlier case law in which "likely" meant "*a degree of probability where there is a very significant and weighty chance ... such that there "may very well" be prejudice to those interests, even if the risk falls short of being more probable than not*"³, and concluded that "*It suffices for it to be likely that substantial distress or damage should be caused. At the same time of course it is insufficient to point to such consequences being a mere possibility.*"

On the facts, the Tribunal was not persuaded that the breach satisfied that test. The fact that the data processor was a specialist contractor with a history of 25-30 years of dealings with the SBC meant that the SBC had good reason to trust the company, and the Tribunal was unable to establish a likely chain of events which would lead to substantial damage or distress. While what did happen was startling, it was a surprising outcome, not a likely one.

³ R(Lord) v Secretary of State for the Home Department (2003) WHC 2073 (Admin.) paras. 99-100.

Client Alert

The Tribunal was not prepared to accept, for example, the suggestion that it was likely that a newspaper would want to publish extracts from the discarded files, given that it was not likely that a newspaper would have obtained them in the first place, nor did it consider identity fraud a likely consequence of the breach.

Notwithstanding this conclusion, at the time of its preliminary decision, the Tribunal was not prepared to simply allow the SBC's appeal. Given the seriousness of its concerns regarding the SBC's procedures in relation to data processing contracts, it postponed consideration of whether to substitute another notice or decision, until such time as a conversation had taken place between the SBC and the ICO regarding the establishment of data processing contracts and the training given to staff involved.

In its final decision notice dated 26 September 2013, the Tribunal stated that negotiations between the SBC and the ICO resulted in agreement, so there was no need to issue an enforcement notice and the SBC's appeal was allowed. The implication of this statement is that the ICO will not appeal the Tribunal's decision, although the ICO has as yet not published any response.

UNFINISHED BUSINESS

In reaching its decision, the Tribunal remarked that whilst some of the personal data disclosed might have referred to ill health, it did not extend to the "sensitive personal data" to which the DPA gives special protection, and it is unclear whether the Tribunal might have reached a different conclusion in such circumstances.

In addition, the Tribunal left open a series of questions which came up in the course of the appeal, but which it had not been necessary to resolve, including:

- In the context of a "deliberate" breach of the DPA, does the "mens rea" or "guilty mind" go to knowingly breaking the law, or deliberately doing an act which is a breach?
- Can the extent of actual (as opposed to likely) harm caused by a breach of the DPA be reflected in the amount of the penalty or the exercise of the penalty discretion?
- Is the way to account for self-reporting to increase the penalty of a data controller who does not self-report (as opposed to reducing the penalty of one who does)?
- Is the ICO's submission that a data controller who makes an early payment of a fine (entitling it to a 20% discount) "effectively forfeits its right to appeal", an obstacle to access the judiciary?

The Tribunal's decision raises the bar that needs to be met by the ICO in order to impose a fine for a breach of the DPA, and may encourage other organisations to challenge ICO decisions in the future. The ICO will now be required to be more precise in articulating the damage and distress that is likely to flow from a breach. The practical implication may be that the imposition of fines will be reserved largely for breaches involving sensitive personal data, where the likelihood of harm is greater.

Client Alert

Contact:

Amy Collins

44 20 7920 4180

acollins@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the *differences that make us stronger*. *This is MoFo*. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "[*Global Employee Privacy and Data Security Law*](#)," or our free online Privacy Library, please visit: <http://www.mofo.com/privacy--data-security-services/> and "like" us on Facebook at <http://www.facebook.com/MoFoPrivacy>.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.