



20 YEARS
PL&B ANNIVERSARY
1987-2007

UNITED KINGDOM NEWSLETTER

PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Information Commissioner should have compulsory audit powers, says *PL&B* survey

One in three respondents has had personal data stolen and most support stronger penalties for DP breaches. By **Laura Linkomies**.

More than four fifths (84%) of data protection professionals support giving the Information Commissioner compulsory audit powers in their sector, and 75% would support the introduction of a criminal penalty for a major breach of data security. These results are the clearest trends in *PL&B*'s recent survey and are remarkable given the high rate of data losses in the participating organisations. This result shows that even the respondents' own organisations might be subject to these ICO audits and criminal penalties.

The most likely explanation for these views is that the respondents consider themselves to be under-resourced. When asked what single change in their organisation would make them more effective in their jobs, respondents most often said "more resources", "more staff" or "more training". Data protection managers and staff have frequently told *PL&B* that their management needs the shock of being subject to an ICO audit and the introduction and application of criminal penalties before they receive sufficient resources to do a proper job.

Losses of personal data are common

One in three respondents has had personal data stolen in the past 12 months. Within the same time-frame, a quarter (26%) had lost

personal data. In almost half of the cases the loss of personal data was due to the theft of a laptop. Other reasons for data loss were losing an unencrypted disk in transit to other financial institutions, correspondence being misdirected, losing USB sticks, mobile phones, blackberry devices and CDs, or losing customer paperwork from an office.

A plan for data breaches

Two-thirds (67%) of respondents had a plan for data breaches. According to survey responses, the plan consisted of notifying:

1. their staff (68%),
2. their customers (61%),
3. the Information Commissioner (56%) and
4. the Financial Services Authority or similar regulatory body (46%), as well as having a media plan.

Only 12% of the respondents were willing to offer compensation to individuals. Other aspects that were mentioned include data audits, a risk assessment, a free credit report and a monitoring service, and informing partner agencies.

Profile of respondents

The survey was completed by 70 individuals working in various DP roles. These included data protection officer (13%), data protection

Continued on p.3

Issue 36

APRIL 2008

NEWS

2 - Comment

New sanctions on the cards

6 - Data protection news

ICO investigates Phorm targeting online ads to individuals • New consumer protection regulations • ASA tells bank to respect opt-out • Solicitors and accountants prosecuted for failure to notify • ICO stops Heathrow's use of biometric data • BBC loses staff personal data • NHS Trust loses 4,000 records • ICO prosecutes debt company • HMRC appoints data guardians • Thomas receives award • Data sharing provisions should be in primary legislation

9 - FOIA news

Straw confirms FOI extension to private sector • Law Lords hear landmark FOI appeal case • House of Commons appeals to High Court

NEWS

3 - Implications of *Ezsis* case

10 - Revised CCTV code launched

12 - M&S receives Enforcement Notice

13 - EU proposes RFID-use guidelines

MANAGEMENT

17 - Web 2.0 privacy risks

19 - Writing a computer-use policy

LEGISLATION & REGULATION

15 - ICO to impose discretionary fines

EVENTS DIARY

16 - DPA/FOIA training, audit training, PL&B's 21st Annual Conference

**Electronic Versions
of PL&B Newsletters
now Web-enabled**

To allow you to click from
web addresses to websites

**UNITED KINGDOM
newsletter**

ISSUE NO 36

April 2008

EDITORIAL DIRECTOR & PUBLISHER

Stewart H Dresner
stewart@privacylaws.com

EDITOR

Laura Linkomies
laura@privacylaws.com

DEPUTY EDITOR

James Michael
james.michael@privacylaws.com

NEWSLETTER SUBSCRIPTIONS

Glenn Daif-Burns
glenn@privacylaws.com

ISSUE 36 CONTRIBUTORS

Gary Brooks
Solicitor and *PL&B* Consultant

Lucy Fisher
PL&B Correspondent

Asher Dresner
PL&B Correspondent

Dugie Standeford
PL&B Correspondent

Robert Waixel
Data Protection Consultant

PUBLISHED BY

Privacy Laws & Business,
2nd Floor, Monument House,
215 Marsh Road, Pinner,
Middlesex HA5 5NE, UK
Tel: +44 (0)20 8868 9200,
Fax: +44 (0)20 8868 5215
Website: www.privacylaws.com

The *Privacy Laws & Business* United Kingdom Newsletter is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of the newsletter. Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given. No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior permission of the publishers.

Design by ProCreative +44 (0)20 8429 2400
Printed by Hendi +44 (0)20 7336 7300

ISSN 1472 9563

©2008 Privacy Laws & Business



New sanctions on the cards

The Information Commissioner's Office (ICO) is currently lobbying hard to retain Clause 76 of the Criminal Justice and Immigration Bill, which will introduce a custodial sentence for those convicted of existing offences of buying or selling personal data.

Richard Thomas issued a statement on 1 April stating his concern about the "powerful last-ditch efforts to get clause 76 removed from the Criminal Justice and Immigration Bill". He said that if data protection is to be taken seriously, it is vital that the Government and other parties stand firm against any possible amendments.

Thomas's worry is more than justified, as UK organisations have much to improve in their DP compliance. The recent *PL&B* survey reveals that one in three respondents has had personal data stolen in the past 12 months. In the same period, a quarter (26%) had lost personal data. However, more than four-fifths (84%) of data protection professionals support giving the Information Commissioner compulsory audit powers in their sector, and 75% would support the introduction of a criminal penalty for a major breach of data security (p.1).

Another Bill that is going through Parliament is the Regulatory Enforcement and Sanctions Bill, which may introduce discretionary fines for criminal breaches of the Data Protection Act. While the ICO considers this largely ineffective and would favour custodial sentences, the Bill is nevertheless worth watching, as it is part of the Government's "better regulation" policy agenda, which aims to improve and simplify the way legislation is made and enforced (see p.15).

The ICO has stepped up its enforcement action. Read about the Enforcement Notice against Marks & Spencer (p.12) and targeted prosecutions against solicitors and accountants (p.7). Marks & Spencer was offered the option of signing an undertaking, but as the company, shortsightedly, did not want this information to be made public, it was given an Enforcement Notice instead.

In this issue, we advise you on how to write a comprehensive computer-use policy (p.19). We also look at the interpretation of the DPA with regard to subject access. When is the search for data reasonable, proportionate and in compliance with the obligations under the 1998 Act? A recent High Court case opens up new horizons (p.3).

Laura Linkomies, Editor

PRIVACY LAWS & BUSINESS

Contribute to PL&B publications

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on tel: +44 208 868 9200, or e-mail: laura@privacylaws.com.

continued from p.1

manager (13%), privacy manager (6%), privacy lawyer (8%) and a selection of other titles varying from compliance manager to deputy company secretary and legal manager.

While half of respondents told us that their data protection team consisted of only one or two people (50%), there were larger teams too: 5% had 9-12 people working on privacy issues. More than half said that their teams had grown in the past 5 years. Less than half of the respondents had a lawyer in their teams (43%). A minority (7%) had their own auditors, but 36% had their own administrative staff.

Half of the respondents had one small central team with smaller teams/individuals with privacy responsibility in individual business areas. Only 16% had one, big central team. A completely decentralised structure was the case for 8% of respondents, while others worked on their own or under other departments, such as marketing or legal services.

Respondents came from several sectors, the biggest being finance (23%), insurance (11%) and local or central government (14%). Some 18% called themselves a privacy team, 12% a data protection team and the rest either had no team or had titles such as

- information governance and management;
- marketing operations;
- information risk and privacy;
- privacy and information law group;
- global privacy office;
- data protection regional coordinators;

- European legal affairs;
- compliance; and
- records and information management team.

Salaries

By far the most common yearly salary bracket among the respondents and people in their data protection teams was £25,000-£40,000. Looking at salaries of 174 people working in data protection, 38% fell into this group. The next biggest groups had salaries of less than £25,000 (18%) and £41,000-£55,000 (16%). Some 11% received £56,000-£70,000, 11% received £71,000-£100,000, and 6% more than £100,000.

Majority receive little training

Worryingly, 14% said that they receive no training during a calendar year. Some 46% said they receive typically 1-2 days of training a year, and 40% attend several training days a year.

Changes to make them more effective

When asked what single change in their organisations would make them more effective in their jobs, respondents most often said "more resources", "more staff" or "more training". Several also wished for an attitude change in senior management. Other comments included more legal support, more communication, acknowledgement of the importance of records management, BCR implementation, enforceable accountability for other staff, better IT systems to support day-to-day application of the DPA, data privacy

responsibilities at board level, and dedicated resources rather than staff who carry out data protection as well as other roles.

Scope of the job

In terms of the scope of work, four-fifths (79%) dealt with the Privacy and Electronic Communication Regulations as well as the DPA, and nearly a half (46%) also had responsibility for FOI compliance. Other legislation that respondents had to deal with included, for example, laws on data security breaches, international DP laws, the Regulation of Investigatory Powers Act, the common law duty of confidentiality, the Human Rights Act, Gambling Act, the Environmental Information Regulations, the Competition Act, and the Companies Act.

Priorities for the year ahead

The question about the major priority for the next 12 months gathered various responses. The most common response was to raise DP awareness within the organisation and make sure that staff are trained in data protection. Other responses include implementing measures to comply with the SWIFT decision, increasing awareness, ensuring data security, reviewing outsourcing contracts, writing a comprehensive privacy policy, and organising an information/data audit.

INFORMATION

The survey was conducted via the PL&B website in the period from 22 November 2007 to 22 February 2008. Thank you to all respondents!

Implications of the *Ezsias* case: Proportionality may apply to searches of data

A recent High Court case provides welcome guidance to organisations trying to cope with onerous subject access requests. **Gary Brooks** reports.

The right of access to personal data is the most fundamental of all the data protection rights. However, readers will be aware that it is increasingly being used by individuals for purposes which are contrary to the rationale of the EU Data Protection Directive.

Organisations continue to face growing amounts of difficult and wide-ranging subject access requests (SARs) for "all information about me", typically to further a complaint or grievance by the individual against the organisation or simply to cause a nuisance. It is also becoming common

for individuals to submit subject access requests to their (former) employers for the purposes of furthering a claim before the Employment Tribunal as part of an evidence-gathering exercise (or fishing expedition), as was the case with Mr *Ezsias* in this matter.

This type of SAR can place a signif-

icant logistical and administrative burden on the organisation due to the way in which the data is stored (if it is not easily accessible) and the sheer amount of information requested by the individual. As a result, they can be financially very costly to deal with.

The question of how far organisa-

SARs to the Welsh Assembly, the last of which was for “all materials and documents whether in paper or electronic format...memos, letters, notes (including e-mails), records (whatever medium they were recorded in) which are connected to me, any decision, consideration, etc related to me...”

prior decision in *Durant* (as it was bound to do) and it did not cite the regulator’s guidance. It instead held that in almost all cases the disputed information withheld by the Welsh Assembly related to Mr Ezsias’s complaint and not to him as an individual (and so it did not qualify as personal data under *Durant* principles).

On the question of whether the Welsh Assembly was justified in withholding information by restricting the scope of its search, the court held the following:

- The DPA only requires the data controller to carry out a “reasonable and proportionate search” for the information requested, and the Welsh Assembly had satisfied this requirement on the facts. The Assembly’s decision to exclude certain departments from the scope of the search for information was considered to be “reasonable and proportionate”, at least in part because the Assembly was able to satisfy the court that it was unlikely that any other department would hold any personal data relating to Mr Ezsias.
- The judge referred to both the £10 administration fee and the £600 fee limit (the latter is relevant

The Assembly’s decision to exclude certain departments from the scope of the search for information was considered to be “reasonable and proportionate”.

tions have to go in responding to these types of SARs has long been a subject of debate. The judgment in the case of *Ezsias v Welsh Ministers* is significant because it provides welcome guidance on this issue.

Legal background

Section 8(2) of the DPA states that a data controller can refuse to provide personal data to a requester on the grounds of “disproportionate effort”, but this proportionality limitation only applies to the obligation to provide a copy of the information requested. The Information Commissioner’s Office (ICO) has also taken the view that the proportionality argument only applies to the supply of a copy of the data and not to the effort, time and expense involved in the prior activity of searching for the data, which is usually more difficult and time consuming. Further, the ICO has adopted a narrow view of what constitutes disproportionate effort (in terms of the level of difficulty, costs and time involved) in order to vigorously uphold the right of individuals to access their data.

The facts in brief

Mr Ezsias worked as a consultant surgeon in a Welsh hospital and was dismissed from his employment in 2005. In response, he commenced proceedings in the Employment Tribunal on the basis that he was a “whistleblower” and therefore his dismissal was automatically unfair. He wrote to the Welsh Assembly asking them to investigate these matters.

To obtain information to assist in his Employment Tribunal claim, Mr Ezsias then made five wide-ranging

The Welsh Assembly withheld much of the information requested on the basis that it was not his personal data under the DPA. Crucially, the Welsh Assembly restricted the scope of its search for personal data to certain departments. It also provided most of this information after the expiry of the 40 day time limit (there was no dispute between the parties that the response had been out of time).

Mr Ezsias was not happy with the response and considered that the search was insufficient and that he had therefore not been provided with all the

The main issue was whether the outstanding information was “personal data”.

information to which he was entitled. He therefore sought a court order requiring the Welsh Assembly to provide him with the further personal data for the stated purpose of assisting his Employment Tribunal claim. He also claimed damages under section 13 of the DPA for the failure to comply with his request within the time limit.

Judgment

The main issue was whether the outstanding information was “personal data”. The recent revised ICO guidance (based on the approach taken at an EU level by the EU Article 29 Working Party) adopts a broad approach to the concept and seems to depart from the narrow tests established by the Court of Appeal in *Durant*.

However, the court followed the

only to public authorities when complying with subject access requests for unstructured personal data) as giving “some context for reasonableness in the context of [the] search”.

- The Assembly had therefore disclosed all disclosable personal data to the claimant pursuant to the SARs in compliance with the DPA (over 1,000 pages of information had been provided to him).
- The judge recognised that the right of access is freestanding and could be exercised in the context of litigation. However, he stated that the court may exercise its discretion against a claimant using subject access as a litigation tool since the disclosure process under the Civil Procedure Rules is the more appro-

appropriate method of obtaining documents. He explained that the DPA gives a right of access to data, not to disclosure of documents and that Mr Ezsias had not understood this distinction.

- Whilst the Assembly had breached the DPA in failing to disclose the disclosable data within the 40 day time limit, Mr Ezsias had suffered no damage arising from the breach and was therefore not entitled to any compensation.

Legal basis for the decision

At first glance, the decision is a little controversial. There is no express provision in the DPA that allows an organisation to limit its search to what is “reasonable and proportionate” and no explanation was given in the judgment for the legal basis for the finding.

However, the legal basis here is that the judge could be said to have adopted a purposive interpretation to read implied wording into the DPA (which implements the EU Directive). The judge’s reasoning seems to be that it could not have been the intention of the EU legislators or the UK Parliament for the subject access right to place an obligation on data controllers to act in a way which was “unreasonable or disproportionate”.

The author’s view is that the judgment is correct in seeking to confirm that proportionality should apply not just to the supply of a copy of the data but also to the extent to which organisations have to commit time and expense in searching for information. Proportionality is indirectly visible in other important parts of the EU Data Protection Directive and the DPA. For

example, in assessing whether the information qualifies as “data” in the first place, the key issue is that the information must be readily accessible by the data controller, whether by means of a computerised search or via a highly structured manual filing system. Whilst this is proportionality in a slightly different context, it would be contrary to the aims of the Directive if businesses were required to engage in highly laborious and expensive searches for information that is not easily retrievable. The point was made concisely by Mr Justice Laddie in the prior case of *Johnson v The Medical Defence Union*:

“...the data controller is only given a short time [namely 40 days] within which to respond to an access request and that he is only to be paid a fee of £10 for being put to the trouble of

data, when the real difficulty and expense is in locating, retrieving and collating the information in the first place.

What does this mean in practice?

It is important to remember that it is up to the courts to interpret the meaning of the DPA and that the ICO can only offer guidance. There has been no official comment from the ICO on the *Ezsias* case. Despite the fact that the court’s decision is binding on the regulator, it seems that the ICO will not be updating its guidance on subject access in light of this development or changing its approach (at least publicly) but will instead view the judgment as applying just in this particular case.

However, the better view is that the judge was establishing a point of principle here which is of general

What is a reasonable and proportionate search will be a question of fact in each case.

producing the required data. The emphasis is on recovering data which are kept in such a way that they can be recovered quickly and cheaply”.

From the author’s experience, there are rare cases where the same amount of effort and costs arise irrespective of whether the information is provided to the individual by way of a copy or whether the information is made available in some other way, for example by inviting the individual to visit the premises to view the data. In such cases, it would be illogical for proportionality to apply only to the supply of a copy of the

application for data controllers faced with with onerous SARs, albeit in limited circumstances.

What is a reasonable and proportionate search will be a question of fact in each case. It is up to the data controller to set the parameters of what is a reasonable search, and if a particular business area or set of data is to be excluded from the search, the organisation must be able to quantify the potential time, cost and effort involved in deciding not to search the excluded location and provide the data. It is a high threshold, and there will still

CHECKLIST FOR HANDLING A BROAD SUBJECT ACCESS REQUEST

The following practical points should be considered when faced with a broad SAR for “all information about me”:

- 1) Find out what information the individual really wants and define the parameters of the search accordingly. This has always been a useful and legitimate tactic and can result in limiting the range of dates for the search or only searching certain departments or e-mail inboxes, for example.
- 2) There is certainly now greater scope for relying on the disproportionate-effort exemption in a wider context, in other words, for the search activities, as well as the supply of the data, particularly if you are dealing with a persistent requester who is

using the right of access as a litigation weapon. You must, however, quantify in detail the likely cost, time and effort involved in searching for the required information and record this in writing. You must be able to justify why any databases/manual filing systems are excluded from the search (on the basis that they are unlikely to contain personal data or that the costs/effort involved in searching them is disproportionate).

- 3) As for how to interpret “personal data”, the risk-averse controller will follow strictly the ICO’s broader approach to personal data when dealing with subject access requests, given that it is the ICO who the

business has to deal with in the event of an individual complaint.

However, it is perfectly legitimate when dealing with a particularly onerous SAR that is clearly made in the context of a dispute or litigation to adopt a robust, risk-based approach in relation to that information that relates to the broader matter/dispute by arguing that it is not personal data based on *Durant* principles (*Durant* is binding law after all). The ICO is obliged to follow the interpretation of the DPA established by the courts. Obviously, you must be aware that the ICO may disagree and order disclosure after an exchange of arguments/correspondence.

certainly be cases where a reasonable and proportionate search is costly, onerous and time-consuming.

Approaches of courts and ICO diverge

This case is a welcome development for businesses faced with onerous SARs. However, it is not a green light to block requests on the basis that they are “unreasonable” or “disproportionate”. The *Ezsias* principle can only be relied on in the restricted circumstances explained above.

It is clear that the courts are more sympathetic than the ICO to the position of data controllers in cases where the right of subject access is being used to further a separate dispute or claim by the individual. Whilst the right of access will always be a fundamental privacy right, this decision is recognition that something does need to be done in exceptional cases to redress the balance

in favour of data controllers who are sometimes faced with a wholly disproportionate burden where the right of access is being misused. Perhaps reform of the subject-access provisions of the Directive is the preferred way of redressing this balance, as this is not just a UK problem.

More worryingly, this case is further evidence of divergence between the decisions of the courts and those of the Information Commissioner on the interpretation of key concepts in the DPA. The recent decision of the Information Tribunal in the *Yorkshire Forward* case is another good example of this, where the Tribunal applied the narrower *Durant* tests (and not the ICO’s guidance) to overturn an ICO decision on whether the information concerned was personal data. The case, *Harcup v. ICO and Yorkshire Forward*, involved disclosure of names of people who attended corporate hospitality

events (EA/2007/0058, 5 February 2008).

This disparity in approach between the UK courts and the regulator to the interpretation of the DPA is unsatisfactory. To ensure that we don’t deviate further from the approach taken in other EU Member States, UK businesses need greater certainty and consistency of approach from the ICO and the courts both on the vital concept of personal data and also on how far their obligations extend when responding to SARs. A court decision overturning *Durant* and endorsing the ICO’s approach on “personal data” would be a good starting point!

AUTHOR

Gary Brooks is a consultant to Privacy Laws & Business and to others, including law firm Berwin Leighton Paisner. e-mail: gary@dataprotected.co.uk web: www.dataprotected.co.uk

ICO investigates Phorm

Three of the UK’s largest ISPs (Virgin Media, BT and TalkTalk) have agreed to pass on individuals’ private browsing history to an advertising broker, Phorm, which is now subject to scrutiny by the Information Commissioner’s Office (ICO). The problem with the Phorm system is that it has not asked individuals to opt-in.

The ICO released a statement on 4 April: “We have had detailed discussions with Phorm. They assure us that their system does not allow the retention of individual profiles of sites visited and adverts presented, and that they hold no personally identifiable information on web users.

“Indeed, Phorm assert that their system has been designed specifically to allow the appropriate targeting of adverts whilst rigorously protecting the

privacy of web users. They clearly recognise the need to address the concerns raised by a number of individuals and organisations including the Open Rights Group.

“We welcome the efforts they are making to engage with sceptical technical experts and believe that it is only by allowing their technology to be subject to detailed scrutiny by independent technical experts that they will be able to prove their assertions regarding privacy. The ICO strongly supports the use of technology in ways which enhance rather than intrude upon privacy, and plans to produce a report on privacy by design later this year.

“We understand that the technology is not yet in use and that BT intends to run a trial involving around 10,000

broadband users later this month. We have spoken to BT about this trial and they have made clear that unless customers positively opt-in to the trial, their web browsing will not be monitored in order to deliver adverts. BT has also stated that the system does not store personally identifiable information, URLs or IP addresses or retain browsing histories, and that search information is deleted almost immediately and is not retrievable.

“We will continue to maintain close contact with Phorm and BT throughout the trial.

“Clearly the trial should reveal whether this is a service that web users want, whether it is privacy friendly and that users are comfortable with the privacy safeguards put in place by Phorm.”

Privacy Laws & Business recruitment service

Do you need a data protection or freedom of information specialist? Is your organisation thinking of recruiting an experienced person to deal with these issues or to strengthen an existing team?

Privacy Laws & Business will help you select suitable candidates from our list of people looking for new jobs or short-term contracts. Using our extensive international network has already proved to be more cost-efficient for companies than

recruiting through non-specialised recruitment agencies or the media. For further information, visit www.privacylaws.com/recruitment or contact Glenn Daif-Burns on tel: +44 (0)20 8868 9200 or e-mail: glenn@privacylaws.com