January 2004 Newsletter

Welcome to the Act Now Newsletter on Data Protection, Freedom of Information, Privacy and Information Management issues in the Public Sector. 1,599 subscribers on January 1st 2004. Next newsletter April 2004.

This is a text version of the newsletter. You can view a HTML version online at www.actnow.org.uk/jan2004.htm - We recommend this.

If you've received this from a colleague you can subscribe in your own right by logging on to www.actnow.org.uk and choosing Newsletter from the menu. You can also unsubscribe on the same page. Please read the disclaimer and other important information at the end of the newsletter.

In this issue

Data Protection Planes land safely - editorial musings



Data Protection planes land safely.

The title of this section (Thanks to Tim Turner for the concept) refers to the recent bad publicity that the DP act has been receiving. The media aren't interested in a plane landing safely but they are interested when there's a crash. And thanks to Humberside Police, British Gas and a few other stories Data Protection has recently been crashing spectacularly.

Huntley's alleged criminal record was not kept by the Police "because the Data Protection Act did not allow it". This has prompted a review.

British Gas disconnected a couple who later died "because Data Protection didn't allow them to tell Social Services".

A chemist who was attacked in his pharmacy but who managed to track down and identify the assailant and obtain his photo and address which he gave to the police was told he had "breached the Data Protection Act"

All this is built up by the media into stories based on "Data Protection Act harms people".

Strangely outside the UK there doesn't seem to be this hangup.

There have been some brave souls who have defended the Act but the whole issue has been blown out of proportion by organisations blaming the Act for their own poor management. Your task should you choose to accept it is to find out the real facts behind these cases and use them in your training courses to your advantage. At last Data Protection has hit the headlines. Use this to get your message across. There's no such thing as bad publicity. Or is there?

Training Courses

If you aren't ready to run training courses we can help. Act Now Training is offering 19 training courses in the Spring at venues throughout the UK. We have officers from Information Commissioner and Scottish Information Commissioner giving keynote speeches. Most courses cost just £149 and all courses have 4.5 hrs CPD available. See the full programme at www.actnowtraining.co.uk  If you want an in house course we can tailor these to your requirements. Contact us on info@actnow.org.uk

1. Data Protection 2004 AD

The AD stands for After Durant. Major news of the last few weeks is the Durant case which appears to rewrite definitions of what is personal data and what is a relevant filing system. See the full judgement at

http://www.courtservice.gov.uk/judgmentsfiles/j2136/durant-v-fsa.htm

Important sections are 28 and 32. Recent conversations with officers from the Information Commissioner seem to suggest that all guidance will be re-written in the light of the Durant verdict. This can only mean that the balance is swinging in favour of the data controller and away from the individual. Essentially it is not personal data unless there is a biographical element or there is an opinion recorded about an individual. The presence of a name or even address does not render this personal data. No longer is there any reason to supply letters written to an individual under and SAR. It's not personal data related to an individual - it's information relating to their SAR or their complaint. Some individuals have over-reacted to this decision and unilaterally decided that the UK is in breach of the original directive. Guidance from the OIC is available at http://ico-cms.amaze.co.uk/DocumentUploads/151203%20Durant.pdf

Watch this space. This one will run and run…

2. New European Decision about a Swedish Churchwarden

See it here http://www.cr-international.com/docs/2003_ecj_bodil_lindqvist_6_11_2003.pdf

A European Court of Justice decision has recently been made which will be of significance to organisations who use global intranet systems or who rely on a website to promote their business. Bodil Lindqvist. This case establishes that loading personal data onto an Internet page which is stored by a hosting provider established in Europe does not breach the Data Protection Directive.

Mrs Lindqvist was involved with her local parish. She set up an Internet page containing information about Confirmations, including the names of many local parishioners, a description of the work they carried out, hobbies and telephone numbers. She also mentioned that one of her colleagues had injured her foot and was working part time on medical grounds. Mrs Lindqvist had not told her colleagues about these pages nor obtained their consent, nor had she notified the Swedish Data Protection Authority about the processing of this personal data. Mrs Lindqvist was fined approximately €450 for processing personal data in breach of Swedish data protection legislation - in particular not notifying the processing to the Swedish Data Protection Authority, transferring data to countries outside Europe (i.e. loading the data onto an Internet page) and for processing sensitive medical data. She appealed to a higher Swedish Court which asked the ECJ whether Mrs Lindqvist's activities had breached the Data Protection Directive.

Article 25 of the Data Protection Directive states that personal data can only be transferred to a country outside the EEA (called "third countries" under the Directive) if that country can offer an "adequate level of protection". Adequacy is to be assessed in light of all the circumstances; in particular this means looking at the nature of the data, the purpose and duration of the proposed processing operation, the country of origin and country of final destination, the rules of law in force in the country where the data is to be transferred to and the professional rules and security measures which are complied with in that country.

The Court noted that in order to obtain the relevant information, an Internet user in a third country would, initially, have to connect to the Internet and then find the webpages. Mrs Lindqvist's Internet pages would not automatically be sent to people who did not intentionally mean to access them, nor would they directly be transferred to an Internet user who requested them; rather they would be transferred through the infrastructure of the hosting provider where the page was stored.

The ECJ also noted that the Directive contains no provisions concerning use of the Internet. Given the state of development of the Internet at the time the Directive was drawn up, the ECJ concluded that it could not presume that the legislation intended the expression "transfer of data to a third country" to cover the loading by an individual of data onto an Internet page, even if those data are accessible by individuals in third countries. The Court concluded that activities such as those carried out by Mrs Lindqvist did not constitute a transfer of data to a third country provided the hosting provider was established in a European state (even if the provider uses a server outside the EC).

The decision is helpful, but leaves unanswered questions. Most notably, the ECJ did not consider the position of the hosting provider itself, only of the website owner. The prohibition on transfers of personal data outside the EEA could still apply to hosting providers who permit a website containing personal data to be accessed from a third country. Furthermore if an organisation is making sensitive personal data available on the Internet (and this may include photographs), it may still need to obtain the consent of the individuals in order to be able to justify the processing of the data. This decision reverses guidance in the Information Commissioner Website Frequently Asked Questions, which states that "placing personal data on the Internet potentially involves a transfer to any country worldwide".

Finally, the case also confirms that the details posted by Mrs Lindqvist would amount to personal data and that the medical details would be sensitive. It also considers the application of the Directive to churches and similar bodies and the interrelationship of data protection and freedom of expression.

Bodil Lindqvist v Kammaraklagaren, Case C101/01 ECJ 6/11/2003.

3. Local Government Act 2003 Chapter 26, Section 85: Explanatory Notes The Council Tax issue

201. Vacant dwellings: use of council tax information. You thought that you could do it. Now you can lawfully. Recent conversations with the IC officials has elicited the statement that they will be 'standing firm on Council Tax'. Reminds us of other well known 'standing firm on …well you name it'. It produces the ridiculous situation where by if a benefits clerk receives a COA they can lawfully pass it on to other Council Departments but if a Council Tax clerk receives it they cannot. Solution – Rename all your Council Tax clerks to be Benefits clerks. (this is open to discussion…)

202. Billing authorities will collect information about the numbers of empty (vacant) homes in their area which are exempt dwellings for council tax purposes. Many local authorities employ empty property officers whose role is to identify empty homes and develop policies and initiatives to bring them back into use. The presence of empty homes can lead to social, economic and environmental problems (e.g. reduce neighbouring property values, encourage vandalism and increase the pressure on housing stock and land for development).

203. The LGFA 1992 does not contain clear provision allowing information collected pursuant to council tax powers under that Act, to be used for other purposes. The Information Commissioner has issued guidance advising authorities that they cannot use council tax data for other purposes.

204. Section 85 inserts a new paragraph 18A into Schedule 2 to the LGFA 1992 to allow a billing authority to use information it has obtained for the purpose of carrying out its council tax functions for the purpose of identifying vacant dwellings or taking steps to bring vacant dwellings back into use. New subparagraph 18A(2) limits the extent of personal information which may be shared to an individual's name or an address or number (e.g. telephone number) for communicating with him.

205. The Government is conscious that it is arguable that allowing the use for other purposes of personal data collected for council tax purposes may in some circumstances constitute an interference with an individual's right to privacy protected by article 8 of the European Convention on Human Rights. It is considered that any data sharing permitted under section 86 does not interfere with an individual's right to privacy. The data will be used only by the billing authority which collected it and it will be used only for public functions in the public interest. Section 85 does not permit disclosure to third parties such as commercial organisations.

4. Code of Practice on Confidentiality in the NHS

http://www.doh.gov.uk/ipu/confiden/protect/copv3.pdf

5. Dear Customer, a reassuring letter from Barclaycard

What is identity theft?

Identity theft happens when someone uses your personal details without your knowledge. Your details can be obtained from something as simple as copying your credit card number to rifling

through your bin to find statements. However it happens, identity theft can end up with fraudsters spending your money and you suffering emotional distress.

How Barclaycard is helping to protect you

We are leading the industry in looking for better, more efficient ways to protect you from fraud. In 2002, while credit card fraud as a whole grew by 3% we reduced fraud by 30%. ,By working together we can reduce it even further. So during a purchase, we may ask to talk to you to confirm your identity. This is no way a reflection of your credit worthiness. We also try to contact you to immediately if your card is used abroad in an unusual way, to check it's you using your card. And we're currently pioneering a new fraud prevention system. Over 30,000 Barclaycard customers in Northampton have been issued with new "Chip and Pin" cards which require them to enter a 4-digit PIN instead of signing a receipt. When Chip and Pin was introduced in France, it reduced fraud by 80%. And by 2005, it will be available throughout the UK. Home or away, you're safer with Barclaycard.

How can you protect yourself against identity theft?

Take a few simple steps and make it difficult for someone to use your details:
Don't discard transaction slips. Because they display your card number. What you consider rubbish can be useful to fraudsters.
Never offer your card details to someone who phones you out of the blue, even if they claim to be from a reputable company.
Make sure your bank and credit card statements arrive when due, and then keep them somewhere safe.
Arrange to redirect all your post when you move house.
Don't respond to unsolicited emails requesting personal details or financial information.
Don't be tricked into telling anyone your personal details e.g. mother's name, work details or date of birth.
Never disclose your PIN to anyone. You will never be asked by a bank to disclose your PIN.
When using a cash machine or point of sale terminal, be wary of anyone trying to watch you enter your PIN.
Don't let yourself get distracted.

6. Data Sharing & Privacy research

http://ess.ntu.ac.uk/dsp/methods.html

7. From an Act Now staff writer

FoI, DPA, and Durant - Impact on personal privacy

The Freedom of Information Act 2000 (FoI) introduces a general right for the public to be given any information the Council holds. Personal data, as defined by the Data Protection Act 1998 (DPA), is exempt – it will remain private. However that definition excludes certain types of data that might otherwise be considered private. Foreseeing this, FoI amends DPA by extending the definition of personal data and then including it in the category of exempt information.

Thus FoI threatened to make unstructured private data accessible to the public, but extends DPA to protect it. However the revised DPA removes from such data most of the other protections that exist for the "old" classes of data. The purpose of this is to avoid extending the burden of compliance.

Public authority data controllers have very little additional work to do in protecting the "new", unstructured data.

This would be a good thing, and not particularly important, except that a recent judgement ("Durant") has narrowed the original definition in DPA. It has narrowed the definition of personal data and also of "relevant filing system". So, potentially, more personal data (or rather data previously thought to be personal) now falls into the unprotected category.

It also means that what used to be considered third party data found in information about to be disclosed to another data subject, may now not be. If so, it is now not necessary to seek the consent of the third party, with all that that implies.

extending the definition of personal data

S1(1) of DPA now defines five classes of personal data (paraphrased):

computerised data
data intended to be computerised,
manual records in a filing system that provides a degree of access comparable to a computer – known as a "relevant filing system"
data comprising health, education or housing records
unstructured data – ie anything else - held by a public authority.

Protections removed by S 33A of the revised DPA

S 33A, inserted by FoI, removes from class e, unstructured data, most of the protections given by DPA. None of the eight principles apply, except that

Pr 4 data must be accurate, and up-to-date

Pr 6 processing of such data must be confirmed in response to a subject access request, but it need not be located or copied unless the subject describes it first, and the cost is not excessive

the subject can demand correction of errors

It is not clear whether, if data from more than one class is being processed, it is necessary to point out that unstructured data is included. The level of excessive cost will be decided by the Secretary of State.

Further, there is

no right to prevent processing of unstructured data even if it causes damage or distress (under DPA, but other legal remedies may exist)
no need to explain the logic of automated decision-making (curiously – since there can be none)
no right of compensation, except for breaches of the limited rights under 4 or 6 above
no obligation to notify such processing to the Information Commissioner (and so no penalties for failing to do so)
no offence of unlawfully obtaining or disclosing such data
Lastly personnel records are exempt from what's left of principles 4 and 6, and from the prohibitions on direct marketing.
Relevant filing systems

This lack of protection only applies to unstructured data, which might be thought to be small or non-existent in extent (and useless for direct marketing for instance). A Council is a bureaucratic organisation and files of data might be expected to be well structured. However the definition of a relevant filing system has been clarified by a recent judgement.

In Durant v Financial Services Authority the Court of Appeal decided that in order to qualify, a filing system must fulfil certain criteria. The judges envisaged a system that "apes" a computerised system:

"It is clear from those provisions that the intention is to provide, as near as possible, the same standard or sophistication of accessibility to personal data in manual filing systems as to computerised records."

The judges considered a file labelled with Mr Durant's name:

" It contains a variety of different documents stored by date order. There is no more detailed structuring than that… this does not in my judgment satisfy the requirement of structuring anticipated by the statutory provision."

This narrow interpretation of a relevant filing system suggests that we should question whether a manual personnel file, labelled with an employee's name but simply holding a set of documents, is no longer to be considered "structured". If not, then a Council is excused (by S 33A) from its obligations under DPA. This being so, a Council should consider whether it wishes to commit itself as a matter of policy to behaving as if it did still have those obligations. This would mean giving the employee (or re-stating) a right of access to the file, or copies of the documents, ensuring that the information is protected from improper disclosure and making explicit that improper disclosure remains a serious disciplinary offence

On the other hand

Just how well-structured or sophisticated is computer access? Consider a subject access request for CCTV images. These are personal data by virtue of being stored and manipulated by computer. But in identifying the subject's data, it is necessary to watch all the video footage in case he or she appears (where there is no electronic search facility able to recognise a human face). This is the sort of drudgery the judges considered data controllers should not have to go through with manual records.

Or consider if the FSA had scanned all the documents in the "Durant" file and stored them in a computer folder called "Durant". The FSA would know that it might amount to computerised personal data, but could not determine that without sitting and reading it all, and applying the judges' test of personal data, again submitting to the drudgery associated with unstructured data.

So if a manual filing system had a facility for locating specific data comparable to these two – that is to say, it was pretty poor – it would still fulfil the new definition of a relevant filing system.

Perhaps the definition has not been narrowed very much at all.

8. How much information in the world?

http://www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm

9. Removing personal data from Word Documents

http://msdn.microsoft.com/library/default.asp?url=/library/en/dnword2k2/html/odc_ProtectWord.asp

10. The Directive on Privacy and Electronic Communications (2002/58/EC)

http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html

11. Leogate

Prime Minister Tony Blair went to great lengths to protect the privacy of his youngest son. He avoided the MMR issue, he kept the boy's image out of the press then one day his son generously gave President Chirac a signed photo. See the result

http://www.mirror.co.uk/news/allnews/content_objectid=13658738_method=full_siteid=50143_headline=-LE%2DOOPS%2D-name_page.html

12. Smile you're on camera

http://www.kablenet.com/kd.nsf/Frontpage/928563D398FE5A5480256DF20046978C?OpenDocument

13. NHS records

http://www.kablenet.com/kd.nsf/Frontpage/6B6EF89FB7262A6580256DF60039F2F0?OpenDocument

14. Access to Communications Data : The New Law

Local authority officers investigating criminal offences, including benefit fraud, will soon have new powers to obtain communications data. The Home Office recently published the draft Regulation of Investigatory Powers (Communications Data) Order 2003 together with a related code of practice (see www.homeoffice.gov.uk). Like other powers under the Regulation of Investigatory Powers Act 2000 ("RIPA"), before these new powers can be used, there is a requirement to seek authorisation and complete various forms. It is therefore vital that all revenues and benefits staff, who may use these powers, have a good understanding of them.

The powers to access communications data are set out in section 21-25 of RIPA. These were previously the domain of a select group including the police, MI5 and the Inland Revenue. They will now be extended to a total of five hundred other public bodies, including councils. However the legislation restricts access to the types of communications data depending on the nature of the body requesting it and the reason for doing so.

The definition of "communications data" includes information relating to the use of a communications service but does not include the contents of the communication itself. It is broadly split into 3 categories: "traffic data" i.e. where a communication was made from, to whom and when; "service data" i.e. the use made of the service by any person e.g. itemised telephone records; "subscriber data" i.e. any other information that is held or obtained by an operator on a person they provide a service to.

Some public bodies will get access to all types of communications data e.g. police, ambulance service, customs and excise. Local authorities will be restricted to subscriber and service use data and even then only where it is required for the purpose of preventing or detecting crime or preventing disorder. For example, a benefit fraud investigator may be able to get access to an alleged fraudster's mobile telephone bill. As with other RIPA powers, e.g. directed surveillance, there are forms to fill out and strict tests of necessity and proportionality to satisfy.

There are two ways in which communications data may be obtained. Firstly, by an authorisation signed by the authorising officer. In the case of a council this will be the assistant chief officer, assistant head of service, service manager or equivalent. An authorisation provides a legal basis upon which the public body may collect the communications data itself e.g. if a communications service provider was technically unable to collect certain communications data. The second way in which communications data may be obtained is where a notice is served upon the holder of the data, requiring them to comply with the terms of the notice and produce the data.

Agreements are in place between communications service providers and public bodies that provide for cost recovery where a service provider is called upon to provide communications data. RIPA itself allows for payment arrangements to be made in order to compensate holders of communications data for the costs involved in complying with the notices.

The new data access provisions are subject to a statutory code of practice, a draft of which has been published for public consultation. It provides guidance on the procedures that must be followed before access to communications data can take place. RIPA provides that the code is admissible in evidence in criminal and civil proceedings.

The draft code of practice sets out in more detail the application process. For example, it requires in writing:

the reason why obtaining the requested data is considered to be necessary;
an explanation of why obtaining the data constitutes conduct proportionate to what it seeks to achieve;
specifying the individual to whom the data relates and the exact data that is required;

RIPA provides for an Interception of Communications Commissioner whose remit is to provide independent oversight of the use of the powers. It also establishes an independent Tribunal which has full powers to investigate and decide any case within its jurisdiction.

These new powers will increase the armoury of benefit and revenues fraud investigators. The Home Office has stressed the importance of staff training. Local authorities need to act now to ensure that their staff are ready to use these new powers responsibly and lawfully.

15. Direct Marketing: The New Law

The Privacy and Electronic Communications (EC Directive) Regulations 2003 came into force on 11th December 2003 and implement EC Directive 2002/58/EC of the same name. They update the current law in the light of new technologies and in particular ensure that the privacy rules currently applicable to phone and fax services also apply to e-mail and to the use of the Internet.

The new regulations will affect a wide range of organisations and individuals including direct marketers, website and online content businesses, providers of subscriber directories, internet users and anyone who sends or receives commercial communications by e-mail or SMS.

The new regulations carry over those elements of the Telecommunications (Data Protection and Privacy) Regulations 1999 which apply to phone and fax marketing. Therefore it is still unlawful:

To use an automated calling system to transmit marketing material without the prior consent of the subscriber. This covers systems that automatically make telephone calls in order to play a recorded marketing message to recipients.
To make a direct marketing telephone call to an individual where the individual has either told the caller's organisation that he does not wish to receive such calls or he has registered with the Telephone Preference Service.To send a direct marketing fax to an individual unless that individual has previously notified the sender that he does not object
To send a direct marketing fax to anyone, whether individual or corporate body, who has notified the sender previously that he does not wish to receive such faxes or has registered with the Fax Preference Service.
There are also provisions for those instigating direct marketing calls or faxes to give certain information to the recipients.

The main new provision of the regulations concerns the use of unsolicited email and text messaging (SMS) for the purposes of direct marketing. Regulation 22 states that generally these may only be sent where an individual has given his/her explicit prior consent to receiving them However f a customer's details are obtained in the course of a sale of a product or service, the business may then use those details to market its own same or similar products or services to that customer. The Information Commissioner has stated that this latter expression is linked to those products and services about which the customer would reasonably expect to receive information.

Those sending direct marketing e mail or SMS must clearly and distinctly give the customer the opportunity to opt-out easily and free of charge when the details are collected and on any subsequent marketing e-mail.

One fundamental flaw in the new regulations is that e-mails sent to a corporate subscriber fall outside the ambit of the regulations except in so far as there is a requirement to identify the sender and to provide contact details. This means that any marketing e mails sent to an individuals e mail address at work will not be caught only those sent to his/her private home e mail. This will cause some concern to many individuals and employers as a vast amount of junk email is received at work thus clogging up the servers and wasting staff time.

There are a further four new provisions in the regulations:

Anyone who uses cookies and similar tracking devices on their websites must give users certain information and a chance to refuse them. This rule does not apply where the cookie or similar device is used only to enable the transmission of website or other online content or where it is an integral part of an online service which cannot be provided without it.

Regulations 7 and 14 allow for the provision of value added services based on traffic or location data. There is no restriction on the type of services that may be provided as long as subscribers give their consent and are informed of the data processing implications.

Regulation 18 gives subscribers a right to decide whether or not they want to be listed in subscriber directories. Subscribers must be given clear information about the directories in question, including any reverse search-type functions, for which additional specific consent is required.

The Information Commissioner will be able to investigate and issue enforcement notices to individuals or companies who breach the regulations. Failure to comply with an enforcement notice

is a criminal offence and is liable to an unlimited fine. Furthermore, an individual who suffers damage as a result of a breach may also pursue a claim for compensation under regulation 30 and/or section 13 of the Data Protection Act 1998. The Commissioner's office has published guidance on how it intends to regulate the operation of the regulations. This is available at http://www.informationcommissioner.gov.uk.

The new regulations will have implications for solicitors, both as senders and recipients of direct marketing. They will also affect solicitors' business clients who will require advice on the implications for their marketing operations.

Summary

The new Privacy and Electronic Communications (EC Directive) Regulations 2003 :

enables the provision of value added services based on location and traffic data, subject to the consent of subscribers (for example, location based advertising to mobile phone users);
removes the possibility for a subscriber to be charged for exercising the right not to appear in public directories;
introduces new information and consent requirements on entries in publicly available directories, including a requirement that subscribers are informed of all the usage possibilities of publicly available directories - e.g. reverse searching from a telephone number in order to obtain a name and address;
extends controls on unsolicited direct marketing to all forms of electronic communications including unsolicited commercial e-mail (UCE or Spam) and SMS to mobile telephones; UCE and SMS will be subject to a prior consent requirement, so the receiver is required to agree to it in advance, except in the context of an existing customer relationship, where companies may continue to email or SMS to market their own similar products on an 'opt-out' basis;
introduces controls on the use of cookies on websites. Cookies and similar tracking devices will be subject to a new transparency requirement - anyone that employs these kinds of devices must provide information on them and allow subscribers or users to refuse to accept them if they wish.

16. DCA Annual Report on implementation of FOI and Action plan

http://www.dca.gov.uk/foi/imprep/annrep03.pdf
http://www.dca.gov.uk/foi/map/modactplan.htm

17. ICO appoints non exe directors

http://ico-cms.amaze.co.uk/DocumentUploads/171203%20Non-Exec%20directors.pdf

18. ICO FOI training presentation. Well it's a start…

http://www.informationcommissioner.gov.uk/cms/DocumentUploads/FOI%20Training%20Presentation.pdf

19. US spam & other things newsletter

http://www.senseient.com/bytesinbrief/bytes.asp?page=currentbytes

20. Midlands Public Authorities Data Protection Group

21st January 2004, 10:30 Stoke on Trent. A spokeman from DCA will be speaking on FOI other items include Data Sharing and the Durant case. To book your place and have a free lunch contact Alan Stead

21. We have joined up

The two main providers of electronic, one-stop change of address services to councils - the company formerly called ihavemoved.com and the Royal Mail (http://www.royalmail.com) - have joined forces. Two years of talks between the former competitors have culminated in Royal Mail taking a 25 per cent stake in the former ihavemoved.com, which has changed its name to Moving Technologies and its product name to iammoving.com (http://www.iammoving.com).

Moving Technologies says it currently has 45 local council clients using its technology, which allows citizens to inform government departments and other services of their change of address in one fell swoop. "Some 85 per cent of local council data is made up of citizens' addresses," says Francesco Benincasa, the company's chief executive. "Our research shows local authorities could cut some 130 million pounds out of their cost base over three years just by working more efficiently on changes of address."

However, there is currently confusion among local authorities about the potential legal issues raised by change of address services. In September 2002, Shepway District Council (http://www.shepway.gov.uk) in Kent was advised by solicitors Nabarro Nathanson that it could be acting unlawfully if it shared resident change of address data between departments.

Rupert Battcock of Nabarro Nathanson advises local authorities to examine other areas of legislation to find legitimacy for services, such as the Local Government Act of 1972 which confirms the powers of local authorities to do things that are incidental to other activities. He also cites the Local Government Act 2000 which gives councils the power to carry out acts that are in the interests of environmental, social and economic well being.

Paul Boyle of the information rights division at the Department for Constitutional Affairs concurs. "Change of address can be construed as being in the social interests of citizens and in the economic interests of the council, as it makes their processes more efficient," he says. The Department for Constitutional Affairs is due to issue guidance to local authorities in the next few weeks which it says will clear up many of these issues.

23. Regional Networking

In the last year many regional groups with an interest in Information issues have sprung up and thrived. Higher up in this newsletter the Midlands Public Authorities Data Protection Group is advertising an afternoon with quality speakers. Next item is about another region with a strong group. Act Now believe there are many such groups and they deserve recognition. It is our intention to write a feature on Regional groups for next issue. This is why you may have received this issue when you weren't expecting to. If you co-ordinate a regional group that networks and supports your members let us know your website, your organiser. We'll give you free publicity. Email Act Now

24. Yorkshire & Humber DP Forum

If you are working in Data Protection in the public sector this site will interest you. There is a free bulletin board and documents to download. The group has a working party on FOI issues. Over 60 members and quarterly meetings in the region. You can also take advantage of free/discounted

courses. Click on http://groups.msn.com/YorkshiretheHumberDPForum and no you don't have to live in the region.

Training in Information Management issues

Act Now offers a programme of high quality but low cost Training courses at city centre venues throughout the UK or can come to you and deliver training in-house. We can train 50 people at your premises for the price of 2 delegates at an expensive London course. Obtain best value for your organisation. Our speakers work in the public sector and bring up to date expertise to the training courses. Contact Act Now for details.

Act Now is a trading name of Act Now Training Ltd
Selbourne House, 26 Selbourne Avenue, Dewsbury, West Yorkshire, WF12 9PA
Fax 01924-520242,  Email info@actnowtraining.co.uk