ICO Enforcement Action Tracker

2012 - The Year of the Security Breach Fine
Introduction

2012 - The Year of the Security Breach Fine

2012 was the busiest year yet for ICO enforcement actions. It would probably be fair to call 2012 “The Year of the Security Breach Fine”, because of the 25 fines that were imposed on data controllers, 22 were for security breaches. Clearly, this is telling us that a security breach provides the most direct route to the imposition of the toughest sanction within ICO’s regulatory tool kit.

The enforcement cases reviewed here also stand as a stark reminder that data protection law is changing rapidly. Regulation has moved from a “toothless tiger” position only a few years back, to being a real force to be reckoned with and a driver for change. ICO is also getting better at investigations and enforcement; the regulator is gaining massive experience, is up-skilling fast and is a force to be reckoned with. Clearly, this new environment presents us all with many challenges.

This Tracker reveals a number of trends within enforcement. It tells us that the financial penalty regime is used almost as much as non-statutory undertakings. It tells us that while the public sector has been the main focus of enforcement action, the focus is now shifting to the private sector (which has been confirmed by the enforcement activity in 2013). It tells us that an organisation that voluntarily notifies a breach of the Data Protection Act (DPA) to ICO is not given immunity from enforcement (21 of the 25 fines were for self reported breaches).

So, apart from security breaches, what else has been the subject of enforcement action? 2012 saw two fines being imposed for breach of the direct marketing rules within the Privacy and Electronic Communications Regulations (PECR), for bulk SMS spam. A fine was also imposed for breach of the data accuracy rule in the DPA. Breach of the rules on CCTV and subject access formed the basis of a couple of Enforcement Notices, while there was 1 set of undertakings for the holding of excessive personal data. However, there was no enforcement action involving the international data transfer rule, or the cookies rule.

In a fast moving environment like this, it is hard for organisations to keep track of the legal developments. That is why we have created this Enforcement Tracker, to give our clients and contacts ready access to these core resources. Hopefully, the Tracker will help you to deliver change to your organisations, where it is needed.

We are updating the Tracker as every new case is published and we will be releasing regular updates throughout the year. The Tracker is supplemented by regular free seminars and conferences – please see the dates of forthcoming events, on the inside back cover.

If you need help with data protection, data security and privacy law, please make contact for an obligation-free discussion. We have the largest legal team of dedicated experts in Europe, with the skills and experience to cover any requirements. We would be delighted to talk through your issues with you.

We hope that you find the Tracker useful. If you have any comments or suggestions for improvements, we would love to hear from you.

Contacts

Stewart Room
Partner
+44 (0)207 861 4850
stewart.room@ffw.com
@StewartRoom

Antonis Patrikios
Director
+44 (0)207 861 4354
antonis.patrikios@ffw.com
uk.linkedin.com/pub/antonis-patrikios/15/428/393
Analysis

Pie 2 shows that non-statutory undertakings are the most used tool of enforcement, but only just; fines come a very close second. The Enforcement Notice seems to withering on the vine however. Pie 3 tells us that ICO does not like to combine sanctions in individual cases.

Pie 4 shows that public sector fines outweigh private sector fines 4:1. Pie 6 shows that the public sector is also more frequently the subject of undertakings, while Pie 8 shows that the public sector received all the Enforcement Notices. The reason for this imbalance against the public sector is partially explained by Pie 14, which shows that over ¾ of fines were imposed on data controllers who reported breaches to ICO. Most of the public sector has adopted a voluntary breach reporting posture, whereas most of the private sector is free of such obligations. Clearly, ICO can only take action against breaches they are aware of, so the enforcement regime is currently loaded against the public sector. However, Pie 7 shows that all the criminal prosecutions were against the private sector, while Pie 9 shows that of the total enforcement actions, just fewer than 50% were against the private sector. So, it isn’t a one way street.

Looking at the categories of offenders, Pies 10 and 11 show that in the public sector Local Authorities are the single largest group, followed by the NHS and then the police. Pie 12 shows that enforcement of the private sector is more fragmented, with private sector health just in the lead, followed by financial services. However, fines of the private sector are more concentrated, with Pie 13 showing financial services, telecoms and health and social care as the only offenders.

Pies 16 and 17 look at DPA enforcement. The security principle (the 7th principle) is way out in front, ICO regulating a total of 119 instances of failure (one case may concern more than one failure). Pie 17 shows the ways in which the 7th principle is breached, with misdirected communications and theft and loss of data out in front. The principle reasons for failure are human error and a lack of training. Pie 17 also confirms that the encryption problem remains. Pie 18 looks at how communications are misdirected; postal errors are out in front, followed by email, then fax. Pies 5 and 19 confirm that security breaches are the main reason for fines, with 22 out of 25 fines having been imposed for breaches of principle 7 of the DPA in relation to 9 different types of security failure. The same pattern is repeated within the undertakings cases, with security breaches being the reason for all but 1 set of undertakings, as demonstrated by Pie 22.
Monetary Penalty Notices: Breakdown per type of failure

- GFA Principle 7: 22
- GFA Principle 4: 1
- PE Regulations 22 and 23: 2

Enforcement action per sector:

- Undertakings:
  - Public Sector: 15
  - Private Sector: 9
  - Social Enterprise: 1
  - Charity: 2
  - Chartered Institute: 1
  - University: 1

- Enforcement action per sector: Totals
  - Public Sector: 39
  - Private Sector: 20
  - Social Enterprise: 2
  - Charity: 3
  - Chartered Institute: 1
  - University: 1

- Enforcement action per sector: Undertakings
  - Public Sector: 3

Monetary Penalties in public sector: breakdown per type of data controller

- NHS: 6
- Police: 4
- Local Authority: 2
- National Park Authority: 1

Monetary Penalties in private sector: breakdown per type of data controller

- Financial institutions: 2
- Health and social care: 1
- Telecoms: 2
- Self-reported: 21
- Not self-reported: 4

Enforcement Action in Private sector: Breakdown per type of data controller

- Financial institutions: 1
- Health: 5
- catering services: 1
- Property and Real estate: 3
- Telecoms: 3
- Legal services: 1
- Private individuals: 1

Enforcement action in public sector: Breakdown per type of data controller

- NHS: 8
- Police: 4
- Local Authority: 2
- National Park Authority: 1

Monetary Penalty Notices: Self-reporting of breach

- Self-reported: 21
- Not self-reported: 4
ANALYSIS

Enforcement action per statute breached

DPA 1998: breach analysis

Monetary Penalty Notices: breach and failure breakdown (one MPN may concern multiple failures)

Prosecutions: breach and failure breakdown

Enforcement Notices: breach and failure breakdown

Misdirected communications: breakdown by type of communication (across all types of enforcement action)

Undertakings: breach and failure breakdown (one undertaking may concern multiple failures)
## Monetary Penalty Notices

### Data Controller | Date | Fine | Breach |
--- | --- | --- | --- |
1. **London Borough of Lewisham** | 10-Dec-12 | £70,000 | DPA - 7th Principle |
   - Failed to take appropriate technical and organisational measures against accidental loss, Social worker left sensitive documents in a plastic shopping bag on a train, after taking them home to work on. The files, which were later recovered from the rail company’s lost property office, included GP and police reports and allegations of sexual abuse and neglect. |

2. **Devon County Council** | 10-Dec-12 | £90,000 | DPA - 7th Principle |
   - Failed to take appropriate organisational measures against unauthorised processing. Social worker used a previous case as a template for an adoption panel report they were writing, but a copy of the old report was sent out instead of the new one. The mistake revealed personal data of 22 people, including details of alleged criminal offences and mental and physical health. |

3. **Tetrus Telecoms (Mr Niebel)** | 28-Nov-12 | £100,000 | PEC Regulations - Regulations 22 and 23 |
   - Mr Niebel sent millions of unsolicited direct marketing text messages, concealed the company’s identity and failed to provide a valid address for recipients to reply to request that the texts cease being sent. |

### Aggravating Factors

1. **Nature of the contravention** - confidential and sensitive personal data lost for period of 7 days and contravention was particularly serious. |
2. **Effect of the contravention** - potential to disrupt ongoing legal case and interfere with administration of justice and potential for extensive media coverage about the data subjects. |
3. **Impact on data controller** - sufficient financial resources to pay MPN. |

### Mitigating Factors

1. **Nature of the contravention** - no previous similar security breach. |
2. **Effect of the contravention** - no evidence that the file of papers has been further disseminated. |
3. **Behavioural issues** - voluntarily reported to ICO, data controller informed the police/train company and recovered the bag, data controller’s information governance team has been completing a risk assessment of social care departments, fully co-operative with ICO and substantial remedial action taken. |
4. **Impact on data controller** - liability to pay MPN will fall on public purse, significant impact on reputation of data controller and there has been no press coverage to date. |

### Remedial Action taken by Data Controller

Remedial action taken includes: provision of lockable bags, restricted number of unencrypted USB pens to be used in a controlled manner. Data controller is considering a more secure means of accessing sensitive personal data out of the office.
Monetary Penalty Notices

### Misdirected communications - social worker’s report sent to wrong family.

A social worker photocopied and sent part of a report relating to family A to family B due to printing issues. The photocopied report contained confidential and highly sensitive personal data relating to the two parents and their four children.

- **Data Controller:** Plymouth City Council
- **Date:** 22-Nov-12
- **Fine:** £60,000
- **Breach:** DPA - 7th Principle

#### Aggravating Factors
1. Misdirected communications: The report was sent to the wrong family.
2. A social worker photocopied the report.

#### Mitigating Factors
1. The social worker performed an error.
2. The report was not further disseminated.

#### Remedial Action taken by Data Controller
- The data controller introduced a new printing procedure for the Child’s Services Department.
- The data controller ensured that the report was not disseminated further.

### Misdirected communications - sensitive personal data relating to a child was sent to an incorrect individual.

A support assistant intended to send some documents internally to an unrelated external user and did not distinguish on the front of the envelope whether it was internal or external.

- **Data Controller:** Leeds City Council
- **Date:** 16-Nov-12
- **Fine:** £95,000
- **Breach:** DPA - 7th Principle

#### Aggravating Factors
1. Misdirected communications: The support assistant sent documents to an incorrect individual.
2. A support assistant re-used an envelope with the wrong budget code.

#### Mitigating Factors
1. The data controller sent the documents to the wrong external user.
2. The documents were corrected and sent to the intended recipient.

#### Remedial Action taken by Data Controller
- The data controller introduced different budget codes for internal and external documents.
- A training programme on information governance has been introduced for all staff.

---

**Brussels | Düsseldorf | Hamburg | London | Manchester | Munich | Palo Alto | Paris | www.ffw.com**
Monetary Penalty Notices

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Fine</th>
<th>Breach</th>
<th>Apportioning Factors</th>
<th>Mitigating Factors</th>
<th>Remedial Action taken by Data Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prudential</td>
<td>06-Nov-12</td>
<td>£150,000</td>
<td>DPA - 4th Principle</td>
<td>Inaccurate data - funds being paid into wrong account.</td>
<td>The social worker went to the home of the prospective adopters to deliver the reports, but they were out and the package would not fit through the letter-box. The social worker went to the home of the prospective adopters to deliver the reports, but they were out and the package would not fit through the letter-box.</td>
<td>Following the breach, the data controller took steps to improve its processes and staff training to minimise the risk of a recurrence.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>There was a mix-up over the administration of two customers' accounts which led to tens of thousands of pounds, meant for an individual's retirement fund, being transferred to the wrong account.</td>
<td>The data controller has now taken steps to improve its processes and staff training to minimise the risk of a recurrence.</td>
<td></td>
</tr>
<tr>
<td>Stoke-on-Trent City Council</td>
<td>25-Oct-12</td>
<td>£120,000</td>
<td>DPA - 7th Principle</td>
<td>Misdirected communications - information about a child protection case emailed to wrong person. Solicitor employed by data controller working on a child protection case sent 11 emails to wrong email address by mistake. Some of the emails contained confidential and highly sensitive personal data regarding injuries sustained together with medical information. Emails also contained the 'Brief to Counsel', directions and comments about conduct of the case. Solicitor was acting in breach of data controller's email and information protection policies as the emails should have been sent via the secure network or encrypted.</td>
<td>Solicitor employed by data controller working on a child protection case sent 11 emails to wrong email address by mistake. Some of the emails contained confidential and highly sensitive personal data regarding injuries sustained together with medical information. Emails also contained the 'Brief to Counsel', directions and comments about conduct of the case. Solicitor was acting in breach of data controller's email and information protection policies as the emails should have been sent via the secure network or encrypted.</td>
<td>Following the breach, the data controller ensured all emails containing sensitive personal data are password protected.</td>
</tr>
<tr>
<td>Prudential</td>
<td>06-Nov-12</td>
<td>£120,000</td>
<td>DPA - 7th Principle</td>
<td>Misdirected communications - information about a child protection case emailed to wrong person. Solicitor employed by data controller working on a child protection case sent 11 emails to wrong email address by mistake. Some of the emails contained confidential and highly sensitive personal data regarding injuries sustained together with medical information. Emails also contained the 'Brief to Counsel', directions and comments about conduct of the case. Solicitor was acting in breach of data controller's email and information protection policies as the emails should have been sent via the secure network or encrypted.</td>
<td>Solicitor employed by data controller working on a child protection case sent 11 emails to wrong email address by mistake. Some of the emails contained confidential and highly sensitive personal data regarding injuries sustained together with medical information. Emails also contained the 'Brief to Counsel', directions and comments about conduct of the case. Solicitor was acting in breach of data controller's email and information protection policies as the emails should have been sent via the secure network or encrypted.</td>
<td>Following the breach, the data controller ensured all emails containing sensitive personal data are password protected.</td>
</tr>
<tr>
<td>Greater Manchester Police</td>
<td>16-Oct-12</td>
<td>£150,000</td>
<td>Unencrypted portable media - theft of unencrypted memory stick.</td>
<td>An officer employed by the data controller had his house burgled resulting in the theft of a personal USB stick kept in his wallet. The USB stick was unencrypted and had no password protection. None of the stolen items have been recovered. The officer had worked for 10 years in Serious Crime Division and downloaded information onto the USB stick. It contained personal data (some sensitive) of approximately 1,075 individuals stored over an 11 year period.</td>
<td>An officer employed by the data controller had his house burgled resulting in the theft of a personal USB stick kept in his wallet. The USB stick was unencrypted and had no password protection. None of the stolen items have been recovered. The officer had worked for 10 years in Serious Crime Division and downloaded information onto the USB stick. It contained personal data (some sensitive) of approximately 1,075 individuals stored over an 11 year period.</td>
<td>Following the breach, the data controller ensured all emails containing sensitive personal data are password protected.</td>
</tr>
<tr>
<td>Norwood Homes Limited</td>
<td>10-Oct-12</td>
<td>£70,000</td>
<td>DPA - 7th Principle</td>
<td>Children's care reports left outside and lost. Social worker employed by data controller obtained two local authorities' background reports relating to four children in care, to inform the prospective adopters of any potential issues. The social worker went to the home of the prospective adopters to deliver the reports, but they were out and the package would not fit through the letter-box. So the social worker called the adopters to inform them she had left the package in a conserved area at the side of the house. When the prospective adopters returned home, the package had not been recovered. The reports contained detailed, confidential and highly sensitive personal data relating to the children and their birth families. The reports have not been recovered and the data controller had not kept copies.</td>
<td>Children's care reports left outside and lost. Social worker employed by data controller obtained two local authorities' background reports relating to four children in care, to inform the prospective adopters of any potential issues. The social worker went to the home of the prospective adopters to deliver the reports, but they were out and the package would not fit through the letter-box. So the social worker called the adopters to inform them she had left the package in a conserved area at the side of the house. When the prospective adopters returned home, the package had not been recovered. The reports contained detailed, confidential and highly sensitive personal data relating to the children and their birth families. The reports have not been recovered and the data controller had not kept copies.</td>
<td>Following the breach, the data controller ensured all emails containing sensitive personal data are password protected.</td>
</tr>
</tbody>
</table>
**Monetary Penalty Notices**

### Scottish Borders Council

**Date:** 18-Sep-12  
**Fine:** £250,000  
**Breach:** DPA - 7th Principle

Pension records found in recycle bin.

Since 2005, the data processor had been digitising pension records of the data controller's past employees/former members of pension scheme - there was no contract in place. A member of the public noticed that a paper recycling bank had been overflowed with discarded files. Some of the files contained personal data and so were handed over to the police. Eight boxes containing 676 files had been deposited in the recycling bank by the data processor. The files contained information including name, address, NI number, date of birth, salary details, bank account details.

### Torbay Care Trust

**Date:** 06-Aug-12  
**Fine:** £175,000  
**Breach:** DPA - 7th Principle

Sensitive information published on Trust's website.

A asked B for equality and diversity metrics held on the electronic staff records system. Two letters were mistakenly sent by post to an address. Those letters contained confidential and highly sensitive personal data. The data subjects in question had not resided at the address the letters were sent to for nearly five years. The breach occurred because the two systems (iClip and SPINE) containing patients details had not been aligned. Furthermore, the staff involved in sending the letters had not received appropriate training and had not verbally checked the address with the data subjects and bypassed a function in the iClip system.

### St George's Healthcare NHS Trust

**Date:** 12-Jul-12  
**Fine:** £60,000  
**Breach:** DPA - 7th Principle

Misdirected communications - medical records sent to wrong address.

Two letters were mistakenly sent by post to an address. Those letters contained confidential and highly sensitive personal data. The data subjects in question had not resided at the address the letters were sent to for nearly five years. The breach occurred because the two systems (iClip and SPINE) containing patients details had not been aligned. Furthermore, the staff involved in sending the letters had not received appropriate training and had not verbally checked the address with the data subjects and bypassed a function in the iClip system.

### Welcome Financial Services Limited

**Date:** 05-Jul-12  
**Fine:** £150,000  
**Breach:** DPA - 7th Principle

Data of more than half a million customers lost.

Business divisions of the data controller maintain back-ups of Local Area Network (LAN) for each business day. The capacity of the storage media meant that each tape could only hold two complete back-ups. After a back-up was made the tapes were transported to an offsite secure IT room. There were 200 tapes in use, each labelled sequentially and these tapes were then re-used when further back-ups were made. It was discovered that 2 unencrypted tapes were missing and contained personal data relating to approximately 20,000 current and former employees during the period 2002 to 2010. There was also personal data relating to approximately 8,000 agents for the same period. There was also customer records relating to approximately 194 million customers. The tapes have not been recovered.

---

### Appraising Factors

1. Nature of the contravention - particularly serious due to confidential nature of personal data, contravention had occurred since 2005 and data processor was free to have disposed of documents in an even less secure manner.
2. Effect of the contravention - affected a maximum of 848 individuals although another 8,000 pension records were potentially at risk and contravention could result in identity fraud and possible financial loss.
3. Impact on data controller - sufficient financial resources to pay MPN up to maximum without causing undue financial hardship.

### Mitigating Factors

1. Nature of the contravention - no previous similar security breach.
2. Effect of the contravention - no complaints from data subjects received to date.
3. Behavioural issues - voluntarily reported, data subjects were notified about security breach, given an apology and offered support/compensation, full investigation carried out, remedial action taken and fully co-operative with ICO.
4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

### Remedy Action Taken by Data Controller

As soon as the data controller was aware of the breach, the spreadsheet was removed from its website and all cached information was deleted by a third party. Remedial action taken includes the implementation of a formal process governing requests for information from the electronic staff records system together with a management of website policy.

---

The data controller terminated the arrangement with the data processor as soon as the breach was discovered.

**Monetary Penalty Notices**

---

**Data Controller** | **Date** | **Fine** | **Breach**
--- | --- | --- | ---
Scottish Borders Council | 18-Sep-12 | £250,000 | DPA - 7th Principle
Torbay Care Trust | 06-Aug-12 | £175,000 | DPA - 7th Principle
St George's Healthcare NHS Trust | 12-Jul-12 | £60,000 | DPA - 7th Principle
Welcome Financial Services Limited | 05-Jul-12 | £150,000 | DPA - 7th Principle
Monetary Penalty Notices

Data Controller | Date       | Fine   | Breach                        | Aggravating Factors                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Mitigating Factors                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Remedial Action taken by Data Controller                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
---|-----------|-------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
**15** Belfast Health and Social Care Trust | 19-Jun-12 | £225,000 | DPA - 7th Principle | 1. Nature of the contravention - serious because of the confidential and sensitive nature of the personal data and it took nearly 4 years to fully decommission the site. 2. Effect of the contravention - large amount of confidential personal data was held on site relating to hundreds of thousands of patients and staff, contravention was likely to cause substantial distress to the data subjects and complaints were made by some of the affected individuals. 3. Behavioural issues - security breaches were not reported to the ICO and contravention was due to negligent behaviour of data controller failing to take appropriate technical/organisational measures to prevent accidental loss of personal data. 4. Impact on data controller - sufficient financial resources to pay a MPN without causing undue financial hardship.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 1. Nature of the contravention - site was extensive, there were concerns about asbestos, contamination and a suspension order was in force for approximately 3 months. 2. Effect of the contravention - no evidence that records have been further disseminated. 3. Behavioural issues - remedial action taken and fully co-operative with Commissioner. 4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | The data controller has taken remedial action which included removing the records from the site, examining them and either retaining or securely disposing of the records. In addition, a Decommissioning Policy to prevent a recurrence was implemented on 6 June 2011.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
**16** Telford & Wrekin Council | 06-Jun-12 | £90,000 | DPA - 7th Principle | Misdirected communications - Social Care Assessment sent to a child's sibling rather than their mother. 1. A staff member sent a Social Care Assessment to two children by post to the wrong individuals. The assessment contained confidential and highly sensitive personal data. The staff member then used the Protocol system incorrectly and failed to check the addresses were correct a second time. 2. Effect of the contravention - 2 of the affected data subjects were moved to alternative foster care placements in the early stages of the investigation. Subsequently, a new Adoption Order was registered and potential for extensive media coverage. 3. Behavioural issues - data controller failed to take sufficient remedial action following the first incident. 4. Impact on data controller - sufficient financial resources to pay a MPN without causing undue financial hardship.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 1. Nature of the contravention - personal data disclosed to unauthorised third parties and contravention was serious because of the highly confidential/sensitive nature of the personal data. 2. Effect of the contravention - 2 similar security breaches were not reported to the ICO and contravention was due to negligent behaviour of data controller failing to take appropriate technical/organisational measures to prevent accidental loss of personal data. 3. Behavioural issues - voluntarily reported, detailed investigation report compiled, full co-operation with the Commissioner. 4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | The data controller has taken remedial action which included providing staff with further training and support on data protection and information security and on using the Protocol system, introducing formal guidance on checking documents printed off the Protocol system and making changes to its configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
**17** Brighton and Sussex Partnership NHS Trust | 01-Jun-12 | £325,000 | DPA - 7th Principle | Inappropriate disposal of IT equipment - hard drives containing sensitive data sold on the internet. 1. Data controller decommissioned a number of hard drives which were kept in commercial storage in a locked room protected by CCTV. Approximately 1,000 of the old hard drives were moved and stored in a room only accessible by using a key code, pending their destruction. The data controller was not aware that an individual had been instructed to destroy the hard drives stored at the hospital. A certificate of destruction was not provided. 2. Effect of the contravention - huge amount of personal data held on 1,000 hard drives relating to tens of thousands of patients and staff. 3. Impact on data controller - sufficient financial resources to pay a MPN without causing undue financial hardship.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 1. Nature of the contravention - no previous similar security breach, security breach was relatively contained and contravention was exacerbated by circumstances outside the direct control of the data controller. 2. Effect of the contravention - 232 hard drives known to have been sold on the internet have all been accounted for, although not all of the drives have been recovered. 3. Behavioural issues - HSS expected to be familiar with nature of personal data in question and need for appropriate security, active attempts made by data controller to recover sold hard drives and assist police in investigation, initial loss voluntarily reported to ICO, detailed investigation report compiled, remedial action taken, data controller may consider an audit and fully co-operative with ICO. 4. Impact on data controller - liability to pay MPN falls on public purse and significant impact on reputation of data controller.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | The data controller has taken remedial action including providing a secure central store for hard drives and other media; reviewing the process for setting potential IT suppliers; obtaining the services of a fully accredited ISO 27001 IT waste disposal company and making progress towards central network access.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

---

1. Nature of the contravention - serious because of the confidential and sensitive nature of the personal data and it took nearly 4 years to fully decommission the site. 2. Effect of the contravention - large amount of confidential personal data was held on site relating to hundreds of thousands of patients and staff, contravention was likely to cause substantial distress to the data subjects and complaints were made by some of the affected individuals. 3. Behavioural issues - security breaches were not reported to the ICO and contravention was due to negligent behaviour of data controller failing to take appropriate technical/organisational measures to prevent accidental loss of personal data. 4. Impact on data controller - sufficient financial resources to pay a MPN without causing undue financial hardship.

1. Nature of the contravention - personal data disclosed to unauthorised third parties and contravention was serious because of the highly confidential/sensitive nature of the personal data. 2. Effect of the contravention - 2 similar security breaches were not reported to the ICO and contravention was due to negligent behaviour of data controller failing to take appropriate technical/organisational measures to prevent accidental loss of personal data. 3. Behavioural issues - voluntarily reported, detailed investigation report compiled, full co-operation with the Commissioner. 4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

1. Nature of the contravention - personal data disclosed to unauthorised third parties and contravention was serious because of the highly confidential/sensitive nature of the personal data. 2. Effect of the contravention - 2 similar security breaches were not reported to the ICO and contravention was due to negligent behaviour of data controller failing to take appropriate technical/organisational measures to prevent accidental loss of personal data. 3. Behavioural issues - voluntarily reported, detailed investigation report compiled, full co-operation with the Commissioner. 4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

1. Nature of the contravention - no previous similar security breach, security breach was relatively contained and contravention was exacerbated by circumstances outside the direct control of the data controller. 2. Effect of the contravention - 232 hard drives known to have been sold on the internet have all been accounted for, although not all of the drives have been recovered. 3. Behavioural issues - HSS expected to be familiar with nature of personal data in question and need for appropriate security, active attempts made by data controller to recover sold hard drives and assist police in investigation, initial loss voluntarily reported to ICO, detailed investigation report compiled, remedial action taken, data controller may consider an audit and fully co-operative with ICO. 4. Impact on data controller - liability to pay MPN falls on public purse and significant impact on reputation of data controller.

1. Nature of the contravention - site was extensive, there were concerns about asbestos, contamination and a suspension order was in force for approximately 3 months. 2. Effect of the contravention - no evidence that records have been further disseminated. 3. Behavioural issues - remedial action taken and fully co-operative with Commissioner. 4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

1. Nature of the contravention - personal data disclosed to unauthorised third parties and contravention was serious because of the highly confidential/sensitive nature of the personal data. 2. Effect of the contravention - 2 similar security breaches were not reported to the ICO and contravention was due to negligent behaviour of data controller failing to take appropriate technical/organisational measures to prevent accidental loss of personal data. 3. Behavioural issues - voluntarily reported, detailed investigation report compiled, full co-operation with the Commissioner. 4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

1. Nature of the contravention - no previous similar security breach, security breach was relatively contained and contravention was exacerbated by circumstances outside the direct control of the data controller. 2. Effect of the contravention - 232 hard drives known to have been sold on the internet have all been accounted for, although not all of the drives have been recovered. 3. Behavioural issues - HSS expected to be familiar with nature of personal data in question and need for appropriate security, active attempts made by data controller to recover sold hard drives and assist police in investigation, initial loss voluntarily reported to ICO, detailed investigation report compiled, remedial action taken, data controller may consider an audit and fully co-operative with ICO. 4. Impact on data controller - liability to pay MPN falls on public purse and significant impact on reputation of data controller.

1. Nature of the contravention - site was extensive, there were concerns about asbestos, contamination and a suspension order was in force for approximately 3 months. 2. Effect of the contravention - no evidence that records have been further disseminated. 3. Behavioural issues - remedial action taken and fully co-operative with Commissioner. 4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

1. Nature of the contravention - no previous similar security breach, security breach was relatively contained and contravention was exacerbated by circumstances outside the direct control of the data controller. 2. Effect of the contravention - 232 hard drives known to have been sold on the internet have all been accounted for, although not all of the drives have been recovered. 3. Behavioural issues - HSS expected to be familiar with nature of personal data in question and need for appropriate security, active attempts made by data controller to recover sold hard drives and assist police in investigation, initial loss voluntarily reported to ICO, detailed investigation report compiled, remedial action taken, data controller may consider an audit and fully co-operative with ICO. 4. Impact on data controller - liability to pay MPN falls on public purse and significant impact on reputation of data controller.

1. Nature of the contravention - site was extensive, there were concerns about asbestos, contamination and a suspension order was in force for approximately 3 months. 2. Effect of the contravention - no evidence that records have been further disseminated. 3. Behavioural issues - remedial action taken and fully co-operative with Commissioner. 4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

1. Nature of the contravention - site was extensive, there were concerns about asbestos, contamination and a suspension order was in force for approximately 3 months. 2. Effect of the contravention - no evidence that records have been further disseminated. 3. Behavioural issues - remedial action taken and fully co-operative with Commissioner. 4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.
# Monetary Penalty Notices

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Fine</th>
<th>Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central London Community Healthcare NHS Trust</td>
<td>21-May-12</td>
<td>£90,000</td>
<td>Misdirected communications - sending faxes to incorrect number. An administrator received a request to send inpatient lists to an additional fax number to ensure service provision was unaffected during the leave of absence of one of the out of hours doctors. The administrator created a fax coversheet listing both numbers. A fax protocol was agreed but the administrator did not update the fax protocol with the second number or obtain approval from a manager. The administrator sent the inpatient lists to the second fax number. A member of the public reported that they had been receiving the inpatient lists but had shredded them. The caller could not be traced.</td>
</tr>
<tr>
<td>London Borough of Birstol</td>
<td>15-May-12</td>
<td>£70,000</td>
<td>Document mishandling - theft of laptop during burglary containing sensitive data. A social worker employed by data controller took home paper records containing confidential personal data. The paper records were kept in social worker’s laptop bag along with an encrypted computer. The social worker’s home was burgled and the laptop paper and all of its contents stolen. The stolen contents have not been recovered.</td>
</tr>
<tr>
<td>Aneurin Bevan Health Board</td>
<td>30-Apr-12</td>
<td>£70,000</td>
<td>Misdirected communications - medical report posted to wrong address. A secretary sent a letter intended for one patient, to a former patient who had an almost identical surname. The secretary simply relied on the electronic patient record system to provide details of the patient. The letter contained confidential information including a report detailing contacts with the patient over a period of 5/6 months.</td>
</tr>
</tbody>
</table>

## Aggravating Factors

1. Nature of the contravention - confidential/sensitive personal data was disclosed to an unauthorised third party and the contravention was serious because of sensitive nature of the personal data.
2. Effect of the contravention - unintended recipient could not be traced and the contravention was likely to cause substantial distress to the data subjects.
3. Behavioural issues - contravention was due to negligent behaviour of the data controller in failing to take appropriate technical/organisational measures against unauthorised processing of personal data.
4. Impact on data controller - sufficient financial resources to pay MPN without causing undue financial hardship.

## Mitigating Factors

1. Nature of the contravention - no previous similar security breach and the personal data involved has not been further disseminated.
2. Effect of the contravention - unintended recipient informed data controller that he had destroyed the inpatient lists.
3. Behavioural issues - voluntarily reported to the Commissioner, data subjects/representatives were notified, detailed investigation report was compiled, substantial remedial action taken and fully co-operative with the Commissioner.
4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

## Remedial Action taken by Data Controller

1. Nature of the contravention - no evidence to suggest personal data has been inappropriately processed and no complaints received from data subjects.
2. Behavioural issues - agreed to ICO audit prior to security breach, voluntarily reported to the Commissioner, data controller fully co-operative, data controller informed the data subjects, full investigation carried out and some remedial action taken.
3. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

The data controller has taken substantial remedial action including not sending inpatient lists by fax, carrying out a detailed internal investigation into the breach and considering the use of more secure means available for sending confidential and sensitive personal data such as email.
Monetary Penalty Notices

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Fine</th>
<th>Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lancashire Constabulary</td>
<td>14-Mar-12</td>
<td>£70,000</td>
<td>DPA - 7th Principle Document mishandling - police file dropped in street.</td>
</tr>
<tr>
<td>Cheshire East Council</td>
<td>15-Feb-12</td>
<td>£80,000</td>
<td>DPA - 7th Principle Misdirected communications - email sent to wrong distribution list.</td>
</tr>
<tr>
<td>Crayon Council</td>
<td>15-Feb-12</td>
<td>£100,000</td>
<td>DPA - 7th Principle Document mishandling - bag stolen from pub, containing social worker’s files.</td>
</tr>
</tbody>
</table>

**Data Controller**

- **Lancashire Constabulary**
  - Date: 14-Mar-12
  - Fine: £70,000

- **Cheshire East Council**
  - Date: 15-Feb-12
  - Fine: £80,000
  - Breach: DPA - 7th Principle Misdirected communications - email sent to wrong distribution list.

- **Crayon Council**
  - Date: 15-Feb-12
  - Fine: £100,000
  - Breach: DPA - 7th Principle Document mishandling - bag stolen from pub, containing social worker’s files.

### Monetary Penalty Notices

#### 1. Nature of the contravention - sensitive personal data relating to approximately 15 data subjects was accidentally lost and hand delivered to a local newspaper and the contravention was serious because of the sensitive nature of the personal data.

- **2. Effect of the contravention** - likely to cause substantial distress to the data subjects.
- **3. Behavioural issues** - contravention was due to the negligent behaviour of the data controller failing to take appropriate organisational measures against accidental loss of personal data.
- **4. Impact on data controller** - data controller is a public authority so liability to pay MPN does not fall on an individual.

#### 1. Nature of the contravention - sensitive personal data relating to one individual disclosed to 180 unintended recipients and contravention was serious because of the sensitive nature of personal data.

- **2. Effect of the contravention** - likely to cause substantial distress to the data subject.
- **3. Behavioural issues** - lack of appropriate data protection training and support and contravention was due to negligent behaviour of the data controller in failing to take appropriate measures against unauthorised processing of personal data.
- **4. Impact on data controller** - sufficient financial resources to pay MPN without causing undue financial hardship.

#### 1. Nature of the contravention - officers routinely handle sensitive personal data and no previous similar security breach and the personal data involved has not been further disseminated.

- **2. Effect of the contravention** - report has been recovered by the police, the data subject and her family were informed and offered ongoing support and no complaints have been received.
- **3. Behavioural issues** - agreed to an ICO audit prior to security breach, voluntarily reported to the Commissioner, detailed investigation report compiled, committed to taking remedial action and fully co-operative with the Commissioner.
- **4. Impact on data controller** - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

#### 1. Nature of the contravention - officers have not handled sensitive personal data.

- **2. Effect of the contravention** - attempts made to recall the email but further dissemination and 57% of intended recipients have confirmed that they deleted the information.
- **3. Behavioural issues** - voluntarily reported to the Commissioner, data controller apologised to individual affected, substantial remedial action taken and fully co-operative with the Commissioner.
- **4. Impact on data controller** - liability to pay MPN will fall on public purse and substantial impact on reputation of data controller.

#### 1. Nature of the contravention - officers have not handled sensitive personal data.

- **2. Effect of the contravention** - report has been recovered by the police, the data subject and her family were informed and offered ongoing support and no complaints have been received.
- **3. Behavioural issues** - agreed to an ICO audit prior to security breach, voluntarily reported to the Commissioner, detailed investigation report compiled, committed to taking remedial action and fully co-operative with the Commissioner.
- **4. Impact on data controller** - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

### Monetary Penalty Notices

#### Appraising Factors

- **1. Nature of the contravention** - sensitive personal data relating to approximately 15 data subjects was accidentally lost and hand delivered to a local newspaper and the contravention was serious because of the sensitive nature of the personal data.
- **2. Effect of the contravention** - likely to cause substantial distress to the data subjects.
- **3. Behavioural issues** - contravention was due to the negligent behaviour of the data controller failing to take appropriate technical/organisational measures against accidental loss of personal data.
- **4. Impact on data controller** - sufficient financial resources to pay MPN without causing undue financial hardship.

#### Mitigating Factors

- **1. Nature of the contravention** - first time personal data of that nature disclosed to voluntary sector co-ordinator.
- **2. Effect of the contravention** - attempts made to recall the email and prevent further dissemination and 57% of intended recipients have confirmed that they deleted the information.
- **3. Behavioural issues** - voluntarily reported to the Commissioner, data controller apologised to individual affected, substantial remedial action taken and fully co-operative with the Commissioner.
- **4. Impact on data controller** - liability to pay MPN will fall on public purse and substantial impact on reputation of data controller.

### Remedial Action taken by Data Controller

- The data controller has taken remedial action which includes informing all officers that certain safeguards must be applied when taking documents out of the station, requiring supervisors to monitor staff working practices, ensuring that vehicle checks are carried out weekly, introducing a procedure for recording the location of paper files and setting up a records management working group to implement a records management policy.

- The data controller attempted to recall the emails that were forwarded but the majority are still unidentified. The data controller also sent an email to the intended recipients asking them to delete the original email. Approximately 57% of the unintended recipients have deleted the email.

- The data controller sent an email reminding all staff not to take information out with them socially after work. The data controller has taken remedial action which includes providing staff with refresher training, reminding staff of importance of keeping information secure on a regular basis, making greater use of encrypted laptops and USB pens when taking information out of the office and carrying out a data protection audit.
## Monetary Penalty Notices

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Fine</th>
<th>Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Norfolk County Council</td>
<td>13-Feb-12</td>
<td>£80,000</td>
<td>DPA - 7th Principle</td>
</tr>
<tr>
<td>Midlothian Council</td>
<td>30-Jan-12</td>
<td>£140,000</td>
<td>DPA - 7th Principle</td>
</tr>
</tbody>
</table>

### Misdirected communications - social work reports posted to wrong address.

A social worker in data controller’s department produced a report for a child protection conference. The child’s father did not attend the conference so the social worker decided to deliver a copy to him. The social worker wrote the incorrect address on the envelope. The unintended recipient opened the envelope, read the report and immediately contacted Norfolk Care Connect to report the issue.

### Misdirected communications - social work reports posted to wrong address.

The data controller was informed by an individual that they had received confidential personal data relating to a child. The individual had been sent an agreement concerning the child in error. Then a social worker sent a child review and care plan to the child’s former address of the child’s mother’s partner who may have further disseminated the information.

## Aggravating Factors

1. Nature of the contravention - unauthorised personal data disclosed to a third party, the data related to 3 data subjects and was serious because of the confidential and highly sensitive nature of the personal data.
2. Effect of the contravention - identities of the data subjects were known to unintended recipient, mother and father made a formal complaint to the data controller, some of the personal data is now in the public domain and the contravention was likely to cause substantial distress to the data subjects.
3. Behavioural issues - contravention due to negligent behaviour of data controller in failing to take appropriate organisational measures against unauthorised processing of personal data.
4. Impact on data controller - sufficient financial resources to pay MPN without causing undue financial hardship.

## Mitigating Factors

1. Nature of the contravention - no previous similar security breach.
2. Effect of the contravention - unintended recipient signed an Undertaking not to disclose the information to any third party and the personal data has not been further disseminated.
3. Behavioural issues - voluntarily reported to the Commissioner, detailed investigation report compiled, substantial remedial action taken and fully co-operative with the Commissioner.
4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

## Remedial Action taken by Data Controller

An email was sent to all staff informing them of their responsibilities in relation to sending personal data by email and the postal service. The data controller carried out a full investigation and the social worker concerned was given a management warning. Remedial action to be taken includes ensuring all staff have completed the e-learning course on data protection, providing mandatory refresher training every three years, monitoring staff training and introducing a peer-checking process if the information being sent or delivered contains sensitive personal data.

## Behavioural issues

1. Nature of the contravention - at least five similar security breaches occurred within five months of each other, unauthorised confidential personal data disclosed to unauthorised third parties and contraventions were serious due to sensitive nature of the personal data.
2. Effect of the contravention - in one of the breaches the information may have been further disseminated to other individuals and the contraventions were likely to cause substantial distress to data subjects.
3. Behavioural issues - data controller should have notified the Commissioner after the first security breach, data controller failed to take sufficient remedial action following first security breach and contraventions were due to negligent behaviour of data controller in failing to take appropriate organisational measures to prevent unauthorised processing of data.
4. Impact on data controller - data controller is public authority so liability to pay MPN does not fall on an individual and sufficient financial resources to pay MPN without causing undue financial hardship.

## Impact on reputation of data controller.

At the time of the breaches the data controller had an overarching policy covering data protection, information security and data sharing. The data controller has now taken remedial action which includes recovering the information, providing all staff with a training session, asking all staff to check that data is accurate before sending and providing experienced staff to assist in developing appropriate policies and procedures in relation to future compliance.

## Effect of the contravention

1. Nature of the contravention - unintended recipients in less of the security breaches were health professionals and used to dealing with personal data.
2. Effect of the contravention - data subjects were not informed due to data controller’s assessment that this would cause significant distress and personal data has either been recovered or destroyed.
3. Behavioural issues - voluntarily reported to the Commissioner, detailed investigation report compiled, remedial action taken and fully co-operative with the Commissioner.
4. Impact on data controller - liability to pay MPN will fall on public purse and significant impact on reputation of data controller.

## Error in data controller's database.

There was another incident where the child’s mother’s GP - the child was not registered with the GP and this had not been checked against the data controller’s database. There was another incident where the child’s report was attached to papers of other children and posted to 4 unintended recipients. In addition, a social worker in error sent minutes of a child protection conference to the child’s former address of the child’s mother’s partner who may have further disseminated the information.

## Personal data relating to a child.

The data controller was informed by an individual that they had received confidential personal data relating to a child. The individual had been sent an agreement concerning the child in error. Then a social worker sent a child review and care plan to the child’s former address of the child’s mother’s partner who may have further disseminated the information.
## Enforcement Notices

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Fine</th>
<th>Breach</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stoke-on-Trent City Council</td>
<td>25-Oct-12</td>
<td>25 October 2012 - £120,000</td>
<td>DPA - 7th Principle</td>
<td>The Commissioner was informed of an incident in which emails containing sensitive personal data were sent in error to an incorrect email address. The address to which the data was sent is a valid, live email account and the data controller has been unable to determine whether or not the emails were read or further disseminated. Data controller has contravened the 7th Data Protection Principle and failed to take appropriate measures to ensure security of data.</td>
</tr>
<tr>
<td>Southampton City Council</td>
<td>25-Jul-12</td>
<td>None</td>
<td>DPA - 1st Principle</td>
<td>The Commissioner considered that the data controller’s policy that all licensed taxis/private hire vehicles be fitted with a CCTV system that features an audio recording facility that is in permanent operation was processing personal data unfairly and unlawfully.</td>
</tr>
<tr>
<td>Staffordshire County Council</td>
<td>07-Feb-12</td>
<td>None</td>
<td>DPA - 6th Principle</td>
<td>The Commissioner has considered a request for assessment made by an individual. The request concerned the failure by the data controller to respond within the prescribed period of 40 days to a subject access request. Commissioner is of the view that the data controller failed to inform the individual, without undue delay, whether personal data of which he was the data subject were being processed by it or on its behalf. Furthermore, the data controller failed to communicate to him in an intelligible form such information as may constitute such personal data.</td>
</tr>
</tbody>
</table>

### Enforced Remedial Action

1. Within 35 days of EN, prepare a programme of training for all employees whose job involves handling personal data.
2. By 28 February 2013, ensure that all employees have undertaken the training in (1) and any new employees receive such training at induction and prior to undertaking work without supervision.
3. After date in (2) ensure all employees undergo refresher training in relation to issues in (1) above at intervals of no more than 2 years.
4. Maintain an auditable record showing details of training undertaken by employees.

1. Erase any personal data in the audio recordings that has already been obtained as a result of the policy.
2. Refrain from recording any such personal data in the future.

3. Supply the individual with a copy of the document in Annex 1 within 35 days of the Enforcement Notice.
## Prosecutions

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Tetrus Telecoms</td>
<td>13-Dec-12</td>
<td>This was an 18 month investigation which centred on 840,000 illegal text messages being sent everyday which produced an income of £7,000-£8,000 per day. Niebel and McNeish are facing prosecution for failing to notify that Tetrus Telecoms was processing personal information. Notification is a legal requirement.</td>
</tr>
<tr>
<td>2 London Barrister – Jeanette Hayne</td>
<td>28-Nov-12</td>
<td>Prosecuted by the ICO for failing to notify. Jeanette Hayne pleaded guilty at the hearing but Westminster Magistrates decided to dispose of the case by way of an absolute discharge owing to particular mitigating circumstances.</td>
</tr>
<tr>
<td>3 Mohammed Ali Enayet (owner of The Lime Lounge in Cleveleys)</td>
<td>02-Aug-12</td>
<td>Prosecuted for failing to register his premises' use of CCTV equipment which was regularly collecting the images of people visiting the restaurant. The bar owner ignored 3 letters from the ICO informing him of his need to register and failed to attend an earlier hearing.</td>
</tr>
<tr>
<td>4 SAI Property Investments Limited (trading as IPS Property Services)</td>
<td>30-Mar-12</td>
<td>A letting agent and one of its directors unlawfully obtained details about their tenants from a rogue employee at Slough Borough Council.</td>
</tr>
<tr>
<td>5 Pinchas Braun (of Tottenham)</td>
<td>27-Feb-12</td>
<td>A letting agent who unlawfully tried to obtain details about a tenant’s finances from the DWP. Mr Braun had no authority to access the tenant’s information held by the DWP.</td>
</tr>
<tr>
<td>6 Juliah Kechil (former Health Care Assistant at the Royal Liverpool University Hospital)</td>
<td>12-Jan-12</td>
<td>Former health worker pleaded guilty to unlawfully obtaining patient information by accessing the medical records of 5 members of her ex-husband’s family in order to obtain their new telephone numbers. She accessed the information for her own personal gain without the consent of her employer.</td>
</tr>
</tbody>
</table>

### Enforced Remedial Action

- **MPN served on Christopher Niebel and Gary McNeish on 26 November.**
  - Two MPNs totalling £440,000.
  - N/A

- **Mr Enayet was fined £100 and ordered to pay £250 prosecution costs by Blackpool Magistrates. He will also pay an additional £15 victim surcharge.**
  - Fined £260 for 2 offences under the Act and ordered to pay a £15 victim surcharge and £702.08 prosecution costs. Another director was fined £260 for 2 offences, ordered to pay £15 victim surcharge and £351.03 prosecution costs.

- **Fined £200 and ordered to pay a £15 victim surcharge and £728.60 prosecution costs.**

- **Fined £500 and ordered to pay £1,000 towards prosecution costs and a £15 victim surcharge.**
The data controller indicated that it intended to review its policies and guidance, and would also review training.

1. The data controller shall review and update its policy for the storage and use of personal data, and shall draft a policy on retention and disposal of data - such policies to be approved and operational by 1 March 2013.
2. All staff shall be made aware of the data controller’s policies for storage, use, retention and disposal of personal data and be appropriately trained by no later than 1 May 2013.
3. Compliance with policies shall be appropriately and regularly monitored.
4. The data controller shall implement such other security measures as are appropriate.

The ICO received a report from the data controller explaining that it had inadvertently included personal data in response to a Freedom of Information (FOI) request made by a journalist. The details related to drug offenses and were contained in a spreadsheet.

The likelihood of identification was reduced as the offenders’ names were not included in the spreadsheet. The risk of further disclosure was mitigated by the provider clearing written instructions on the secure storage of hard copy personal data off site for emergency purposes.

1. All FOI responses are double checked, preferably by a manager, to ensure that no personal data is included.
2. A specific written FOI procedure is implemented within the Information Compliance Unit. This should include the requirement to use a set checking procedure and to log all actions.
3. FOI responses are converted to a PDF format whichever possible.
4. Staff are aware of the data controller’s policy for the retention, storage and use of personal data and are appropriately trained how to follow that policy.
5. The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction and/or damage.
**Undertakings**

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Holroyd Howe Independent Ltd.</td>
<td>23-May-12</td>
<td>DPA - 7th Principle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A data processor reported to the Commissioner that it had received a request from one of the data controller’s ex-employees for a copy of one of his payslips. In error, the data processor emailed him a PDF document showing the relevant month’s payslips for all of the data controller’s employees. The Commissioner’s investigation revealed that the data controller did not have a formal contract in place governing the processing of personal data by this data processor. The data controller gave job-related training which included emphasis on confidentiality and sensitivity of data where appropriate.</td>
</tr>
<tr>
<td>Aneurin Bevan Health Board</td>
<td>30-Apr-12</td>
<td>DPA - 7th Principle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Commissioner was provided with a report that a letter containing a detailed psychological report of a mental health patient had been sent to another former patient with a very similar name. The consultant emailed his letter to a secretary for formatting but did not include sufficiently clear identifiers for the secretary to select the correct patient. The Commissioner’s investigations revealed that neither the consultant nor secretary involved in this incident had received any data protection training from the data controller.</td>
</tr>
<tr>
<td>Safe and Secure Insurances Services Limited</td>
<td>25-Apr-12</td>
<td>DPA - 7th Principle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Commissioner became aware that a hard drive purchased from the internet contained personal data relating to the data controller’s clients. The documents mainly consisted of insurance quotes and application forms. The Commissioner’s investigations revealed that the data controller could not confirm how the hard drive had ended up in the public domain. The data controller did not have an adequate data protection policy in place at the time of the incident and did not have a drive disposal procedure. The data controller did not keep a record of any decommissioned equipment.</td>
</tr>
<tr>
<td>Brecon Beacons National Park Authority</td>
<td>18-Apr-12</td>
<td>DPA - 7th Principle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Commissioner was informed by the data controller about two data security incidents which related to the unauthorised disclosure of personal data on the data controller’s website. Both incidents were voluntarily reported to the Commissioner.</td>
</tr>
</tbody>
</table>

**Remedial Action taken by Data Controller**

<table>
<thead>
<tr>
<th>Remedial Action taken by Data Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. All staff are made aware of the data controller’s amended policy for the storage and use of personal data and are appropriately trained on how to follow that policy.</td>
</tr>
<tr>
<td>2. Appropriate security measures are taken to protect personal data sent by email; in particular, sensitive personal data shall not be transmitted by email across the internet unless encrypted to current standards.</td>
</tr>
<tr>
<td>3. Compliance with data controller’s policies on data protection and IT security issues is appropriately and regularly monitored.</td>
</tr>
<tr>
<td>4. The data controller shall enter into formal contracts/agreements with any data processor it selects to process personal data on its behalf.</td>
</tr>
<tr>
<td>5. The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction and/or damage.</td>
</tr>
</tbody>
</table>

**Undertakings**

<table>
<thead>
<tr>
<th>Undertakings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Adequate security measures are put in place to prevent unauthorised access to personal data from the data controller’s website. This includes the redaction of personal data when planning documentation is prepared for publication.</td>
</tr>
<tr>
<td>2. Staff are aware of the data controller’s policy for the retention, storage and use of personal data and are appropriately trained on how to follow that policy.</td>
</tr>
<tr>
<td>3. The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction and/or damage.</td>
</tr>
</tbody>
</table>
## Undertakings

### Undertakings

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10</strong> Leicestershire County Council</td>
<td>17-Apr-12</td>
<td>DPA - 7th Principle</td>
</tr>
<tr>
<td><strong>11</strong> Toshiba Information Systems UK Ltd</td>
<td>17-Apr-12</td>
<td>DPA - 7th Principle</td>
</tr>
<tr>
<td><strong>12</strong> Hertfordshire County Council</td>
<td>18-Apr-12</td>
<td>DPA - 7th Principle</td>
</tr>
<tr>
<td><strong>13</strong> South London Healthcare NHS Trust</td>
<td>18-Apr-12</td>
<td>DPA - 7th Principle</td>
</tr>
</tbody>
</table>

The data controller had recognised the risks associated with home working and had initiated a specific training programme.

The data controller had put in place some policies/procedures and the officer concerned had received relevant training.

1. The data controller will obtain sufficient guarantees from the data processor that it will conduct appropriate web application security tests which the data controller may instruct the data processor to create and which involve the processing of personal data.
2. The data controller shall take reasonable steps to ensure the data processor complies with all such guarantees in processing data for the purposes of Relevant Web Applications.
3. The data controller shall (i) consider data security in instructing the data processor to construct Relevant Web Applications, and (ii) take reasonable steps to ensure the data processor considers data security in constructing those Applications.
4. The data controller shall implement appropriate and proportionate data security testing on each Relevant Web Application prior to launch.
5. The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised or unlawful processing, accidental loss, destruction and/or damage.

1. Where appropriate, portable and mobile devices are to be used to store and transmit personal data and those devices are to be encrypted using encryption software which meets the current standard.
2. Physical security measures are adequate to prevent unauthorised access to personal data.
3. The data controller continues to make staff aware of their revised Data Protection Policy and staff are appropriately trained.
4. Hard copy documentation is only removed from Council premises when absolutely necessary. It will contain the minimum amount of personal data required for its purpose. Compliance with these procedures is regularly monitored.
5. The data controller shall implement all necessary security measures.

1. Existing policies should be amended to include detailed guidance relating to the security of paper documents whilst home working.
2. Staff are made aware of the data controller’s amended policies for the security of personal data and are appropriately trained on how to follow that policy.
3. Appropriate monitoring should be implemented by the data controller to ensure compliance with such policies.
4. The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction and/or damage.

1. Portable/mobile devices are to be encrypted using encryption software which meets the current standard.
2. Physical security measures are adequate to prevent unauthorised access to personal data.
3. The policy covering the storage and use of personal data is followed by all staff.
4. Staff are made aware of the data controller’s policy for the retention, storage and use of personal data and are appropriately trained.
5. The data controller shall implement all necessary security measures.
The Commissioner was informed by the data controller of the theft of a laptop, router and printer in March 2011. The stolen laptop was password protected and software encryption was used. Investigations revealed that neither of the memory sticks were encrypted and there was no specific policy in place to cover working away from the office.

The data controller informed the Commissioner of the theft of a laptop, router and printer in March 2011. The laptop contained personal data relating to at least 20 employees. The stolen laptop was password protected but not encrypted.

The data controller informed the Commissioner of the theft of a laptop, router and printer in March 2011. The laptop contained personal data relating to at least 20 employees. The stolen laptop was password protected but not encrypted.

Immediate and comprehensive remedial action was taken and the use of all removable media devices is now prohibited.

The Commissioner was informed of the theft of a laptop, router and printer in March 2011. The laptop contained personal data relating to at least 20 employees. The stolen laptop was password protected but not encrypted.

The data controller undertook no monitoring to confirm that the training was being conveyed to all staff.

The Commissioner was informed of the theft of a laptop, router and printer in March 2011. The laptop contained personal data relating to at least 20 employees. The stolen laptop was password protected but not encrypted.

The Commissioner was informed of the theft of a laptop, router and printer in March 2011. The laptop contained personal data relating to at least 20 employees. The stolen laptop was password protected but not encrypted.

The data controller undertook no monitoring to confirm that the training was being conveyed to all staff.

The Commissioner was informed of the theft of a laptop, router and printer in March 2011. The laptop contained personal data relating to at least 20 employees. The stolen laptop was password protected but not encrypted.

The data controller undertook no monitoring to confirm that the training was being conveyed to all staff.

The data controller undertook no monitoring to confirm that the training was being conveyed to all staff.

The data controller undertook no monitoring to confirm that the training was being conveyed to all staff.
**Undertakings**

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Breach</th>
<th>Remedial Action taken by Data Controller</th>
</tr>
</thead>
</table>
| **20** Dr Pervinder Sanghera of Arthur House Dental Care | 01-Mar-12 | DPA - 7th Principle | 1. Portable/mobile devices shall be encrypted using encryption software which meets current standards.  
2. Staff shall only take personal data off site where absolutely necessary and shall only use approved mobile devices.  
3. Staff are made aware of the data controller’s policy for the storage/use of personal data and are appropriately trained.  
4. The data controller shall implement appropriate secure back-up solutions for electronic personal data.  
5. The data controller shall implement all other necessary security measures. |
| **21** Fairbridge | 10-Feb-12 | DPA - 7th Principle | Since the incidents the data controller has ensured the encryption of mobile devices that contain personal data and provided all employees with data protection training. |
| **22** Turning Point | 10-Feb-12 | DPA - 7th Principle | There was no formal written policy in place to cover the relocation of files containing personal data. |
| **23** Basingstoke and Deane Borough Council | 10-Feb-12 | DPA - 7th Principle | The Commissioner is satisfied that the data controller will implement suitable remedial steps including the provision of a compulsory data protection e-learning module for all staff. |
| **24** Brighton and Hove Council | 10-Feb-12 | DPA - 7th Principle | The email address used was hidden from other employees and the email was promptly recalled meaning that disclosure was limited. |

**Remedial Action taken by Data Controller**

1. Portable/mobile devices shall be encrypted using encryption software which meets current standards.  
2. Staff shall only take personal data off site where absolutely necessary and shall only use approved mobile devices.  
3. Staff are made aware of the data controller’s policy for the storage/use of personal data and are appropriately trained.  
4. The data controller shall implement appropriate secure back-up solutions for electronic personal data.  
5. The data controller shall implement all other necessary security measures.
Undertakings

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Breach</th>
<th>Undertakings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dacorum Borough Council</td>
<td>10-Feb-12</td>
<td>Data Protection Act - 7th Principle</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Commissioner was notified that a computer hard drive containing</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sensitive personal data was</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>stolen from an adventure playground following a burglary. The</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>computer contained approximately 1,000 registration documents of</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>children who attended the playground. The</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Commissioner’s investigations revealed that no annual review of the</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>database had been performed.</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td>Bolton Council</td>
<td>10-Feb-12</td>
<td>Data Protection Act - 7th Principle</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Commissioner received a report from the data controller about</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a theft of a rucksack from a keyworker’s car. The bag contained</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hard copy documentation featuring sensitive personal data. There was</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>also a second incident involving the loss of data via email.</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Investigations revealed that despite the fact that many employees</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>are predominantly mobile workers, the data controller had</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>not sufficiently explored the implications of handling personal data</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in a mobile environment.</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td>Crawley District Council</td>
<td>10-Feb-12</td>
<td>Data Protection Act - 7th Principle</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Commissioner was informed by the data controller of the theft</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>of an unencrypted laptop containing a database with child swimming</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lesson details for 2,300 individuals.</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td>E*Trade Securities Ltd</td>
<td>03-Feb-12</td>
<td>Data Protection Act - 7th Principle</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Commissioner was informed by the data controller that files</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>containing personal data related to approximately 608 client files</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>placed in storage with a data processor were missing.</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Commissioner’s investigations revealed that the data controller</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>had no contractual agreement with their UK data processor.</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td>Manpower UK Ltd</td>
<td>20-Jan-22</td>
<td>Data Protection Act - 7th Principle</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Commissioner was provided with a report indicating that one of</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the data controller’s employees had emailed a spreadsheet containing</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the personal data of over 400 individuals to 60 employees in error.</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The data controller had not given sufficient consideration to the</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>security of personal data compromised and sent all data to the</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>employee involved. It was also discovered that the data had been</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>transmitted over the internet without protection.</td>
<td>Undertakings Undertakings Undertakings Undertakings Undertakings Undertakings</td>
</tr>
</tbody>
</table>

Remedial Action taken by Data Controller

1. All staff are made aware of the data controller’s amended policy for the storage and use of personal data and are appropriately trained on how to follow that policy.
2. Personal data shall not be retained when no longer relevant or required for its original purpose.
3. Any personal data which is no longer needed shall be disposed of in a secure manner, procedures for which shall be covered in the data controller’s policies and communicated to all relevant staff.
4. The data controller shall implement all other necessary security measures.

The data controller did have policies in place covering removal of personal data from the office and the employee concerned had received appropriate training.

1. Hard copy documentation is only removed from the station when absolutely necessary. It will contain the minimum amount of personal data required and will be anonymised where possible.
2. Thorough risk assessments are completed for all mobile working arrangements.
3. Staff are aware of the data controller’s policies and are appropriately trained.
4. Compliance with the data controller’s policies is appropriately and regularly monitored.
5. The data controller shall implement all other necessary security measures.

None.

The data controller intends to implement a written contractual agreement with its data processor in the future.

1. Any processing of personal data carried out by a data processor on behalf of the data controller is carried out under a written contract.
2. Sufficient guarantees are obtained in respect of technical/organisational security measures provided by the data processor.
3. A detailed audit trail will be maintained.
4. A detailed record of personal data couriered internationally will be maintained in respect of all client personal data.
5. The data controller will take steps to comply with the requirements of the 8th Data Protection Principle.
6. The data controller shall implement all other necessary security measures.

The data controller attempted to contact recipients to request deletion but it has not been possible to confirm this has been done in all cases.

1. All staff are made aware of the data controller’s policy and are appropriately trained.
2. Any personal data transmitted by email over the public internet shall be protected by password/encryption.
3. Compliance with the data controller’s policies is appropriately and regularly monitored.
4. The data controller shall implement all other necessary security measures.
Undertakings

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Date</th>
<th>Breach</th>
<th>Undertakings</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 Chartered Institute of Public Relations</td>
<td>18-Jan-12</td>
<td>DPA - 7th Principle</td>
<td>The Commissioner became aware of an incident involving the loss of up to 30 CIPR membership application forms. Investigations revealed that at the time no written policy was in place to cover working away from the office and several other of the data controller’s procedures for handling personal data were also lacking.</td>
</tr>
</tbody>
</table>
| 31 Praxis Care Limited | 18-Jan-12 | DPA - 3rd Principle  
DPA - 5th Principle  
DPA - 7th Principle | The Commissioners were provided with reports that a unencrypted USB stick used as a backup and transfer device was lost. The device contained sensitive personal data about 107 data subjects on Isle of Man and data about 53 data subjects in Northern Ireland. |
Looking ahead: 2013 and beyond

2013 has got off to a slightly slower start with only two fines at the date of publication of this Tracker. However, our research across our own case files and in conversations with other lawyers suggests that 2013 will be another record year.

While we expect that security breaches will remain the core focus of enforcement activity, there is a good chance that the cases will expand beyond data loss events and encryption problems to cybersecurity. Indeed, one of this year’s fines is a cybersecurity case.

We also expect there to be more enforcement activity against the private sector. The EU regulators are taking coordinated, high profile action against the private sector, based around Privacy Policies, while the PECR compulsory breach notification regime applying to telecommunications companies and ISPs is bound to result in enforcement action at some point. The cookie rule is also hotly tipped to appear within the cases. There is an outside chance that the press and media will get more scrutiny, as a result of the Leveson Inquiry into Phone Hacking. Yet, we don’t expect international transfers to make an appearance any time soon.

There will also be more appeals against fines. The first appeal went to court in December and we know of two others that are in the pipeline. If ICO increases their enforcement activity in the private sector, we expect that will drive forward more appeals, on the basis that the private sector has a greater appetite to challenge enforcement actions.

Looking further ahead, the Draft EU Data Protection Regulation will be a massive driver of enforcement activity. The compulsory breach notification regime will be the principal reason for this, bringing more and more cases to ICO’s attention.

Last, but not least, the Draft EU Cybersecurity Directive (February 2013) shouldn’t be forgotten. This will create a parallel regulatory regime for “market operators”, to force them to become more secure. This will drive its own enforcement activity.

Field Fisher Waterhouse
22 February 2013

About us

A selection of our Privacy and Data Security Events in 2013

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>DG Event: BCR/BCPR Master Class</td>
<td>27 February 2013</td>
<td>All day</td>
</tr>
<tr>
<td>DG Event: Data Breach Intensive</td>
<td>18 March 2013</td>
<td>All day</td>
</tr>
<tr>
<td>Privacy &amp; Data Security Breakfast Briefing</td>
<td>17 April 2013</td>
<td>09:00 – 11:00</td>
</tr>
<tr>
<td>Privacy &amp; Data Security Breakfast Briefing</td>
<td>1 May 2013</td>
<td>09:00 – 11:00</td>
</tr>
<tr>
<td>Security Forum</td>
<td>8 May 2013</td>
<td>All day</td>
</tr>
<tr>
<td>DG Event: Data Protection Regulation</td>
<td>15 May 2013</td>
<td>All day</td>
</tr>
<tr>
<td>Privacy &amp; Data Security Breakfast Briefing</td>
<td>29 May 2013</td>
<td>09:00 – 11:00</td>
</tr>
<tr>
<td>Privacy &amp; Data Security Breakfast Briefing</td>
<td>12 June 2013</td>
<td>09:00 – 11:00</td>
</tr>
<tr>
<td>Privacy &amp; Data Security Breakfast Briefing</td>
<td>26 June 2013</td>
<td>09:00 – 11:00</td>
</tr>
<tr>
<td>Privacy &amp; Data Security Breakfast Briefing</td>
<td>10 July 2013</td>
<td>09:00 – 11:00</td>
</tr>
<tr>
<td>Security Forum</td>
<td>4 July 2013</td>
<td>All day</td>
</tr>
<tr>
<td>Privacy &amp; Data Security Breakfast Briefing</td>
<td>24 July 2013</td>
<td>09:00 – 11:00</td>
</tr>
<tr>
<td>Privacy &amp; Data Security Breakfast Briefing</td>
<td>7 August 2013</td>
<td>09:00 – 11:00</td>
</tr>
</tbody>
</table>

About our Data Security and Privacy Practice

Our market leading Privacy and Information Law Group has specialist knowledge across all areas of data protection, data security, freedom of information, information sharing, confidentiality and human rights law. We carry out data protection audits, devise e-privacy strategies, draft privacy policies, rules and guidelines, advise on dealings with individuals, data protection authorities and other regulatory agencies, global privacy programmes, international transfers of data including the adoption and roll out of Binding Corporate Rules as well as contentious privacy issues.

One of the group’s main focus areas is networks and data security. We regularly advise clients on security breaches and data loss, on how to carry out internal corporate investigations and on how to deal with the regulators and the press. We are unique in that we deal with the contentious aspects of data protection, representing clients in criminal prosecutions, in challenges to regulatory enforcement action and related litigation. We are consistently ranked the number 1 Data Protection practice by the legal directories, Chambers and Legal 500, demonstrating our market leading work and our specialist lawyers.

About Field Fisher Waterhouse

Field Fisher Waterhouse is a European law firm providing commercial solutions across a range of industry sectors. We have a particular focus on companies that are highly regulated and those with intellectual property and technology driven business models. The firm has over 150 partners, 240 other lawyers and nearly 300 support staff across offices in Brussels, Dusseldorf, Hamburg, Paris, London, Munich, Manchester and Palo Alto.