

## Compliance with the Data Protection Act 1998 – 2<sup>nd</sup> Round

### Hampshire Fire and Rescue Authority

#### INSIDE THIS REPORT

##### PAGES 2 - 6

#### Summary

- Introduction
- Scope
- Objectives
- Audit approach
- Main conclusions
- The way forward
- Acknowledgement

##### PAGES 7 - 10

#### Action Plan

##### PAGES 11 - 18

#### Detailed Report

- Preparing for Notification (Section 2)
- Data quality (Section 5)
- Data security (Section 8)



**DISTRICT AUDIT**

---

<b>Reference:</b>	JRHA0090701W.doc – Final
<b>Author:</b>	Ken Adcock
<b>Date:</b>	September 2001

## Introduction

Within the space of twelve months, three items of legislation have come into force that will address the need to protect citizens' rights to privacy and accuracy of information held in the new information environment. The main drive is to provide the citizen with significantly enhanced powers to access information held about them by public bodies and, through the Information Commissioner, to question the security and use made of that information.

These added rights for the citizen create greater obligations on the public sector as a whole to ensure that personal data is identified, notified to the Information Commissioner, is made as reasonably secure as possible and is available to any citizen who is legally entitled to ask for it.

The items of legislation creating these obligations are:

- the Data Protection Act 1998, which came into force on 1 March 2000. There are transitional arrangements which mean that data users have to address a number of tasks by 24 October 2001
- the Freedom of Information Act will also impose certain duties on public health sector bodies, such as the requirement to produce a strategy on publishing information they hold
- the Human Rights Act, enacted in October 2000 may also increase citizens' rights to access information and challenge decisions made based on that information.

As a result of the short timescale for achieving compliance with the Data Protection Act (DPA) by the transition date of 24 October 2001, District Audit has developed a methodology to assess the progress being made by all audited bodies, through the collection of data, to enable comparisons to be made within the relevant client groups. The first round of audit is now nearing completion.

## Scope

It is important to appreciate that, whilst we have reviewed the management arrangements for dealing with compliance with the DPA, it is not within the remit of District Audit to test information security or that the Authority's Notification to the Information Commissioner accurately reflects the Authority's information holdings. The Authority will, however, gain assurance that its arrangements for compliance should ensure that such issues are properly addressed.

## Objectives

The objectives of this review are to:

- identify the management arrangements in place to achieve compliance with the legislation
- review the plans made by the Authority to prepare for Notification of the purposes under which data is processed
- ensure that all actions necessary to deal with Transition to the requirements of the new Act have been identified
- evaluate the robustness of the Authority's data protection management systems
- evaluate, where possible, the robustness of the Authority's policies for ensuring the accuracy and quality of the data

- review the Authority's ability to comply with a data subject access request within 40 days
- review the Authority's procedures and protocols for ensuring legal external transfer of data
- ensure that the Authority's information security policy addresses the requirements of the DPA
- agree a series of action points to be addressed before 24 October 2001.

The criteria listed were the basis of the initial 'baseline' assessment undertaken by District Audit throughout England and Wales between November 2000 and April 2001. The results from these audits will now be used by District Audit to extrapolate changes from the first set of results and thereby assess whether the recommended improvements have been implemented and to determine whether the Authority will be in a position to achieve compliance by 24 October 2001.

## Audit approach

The approach adopted has been as follows:

- review of arrangements involving key members of staff
- review of the current documentation, including guidance to the Authority's employees
- evaluation of the current position of the Authority using a structured scoring mechanism.

This has been followed up through monitoring of progress by comparison with targets, produced by District Audit, after discussions with the Office of the Information Commissioner on matters relating to compliance with the provisions of the 1998 Act.

The scores for each required activity range from '0' where the issue has not been addressed to '3' where the activity has been completed and, where applicable, documented.

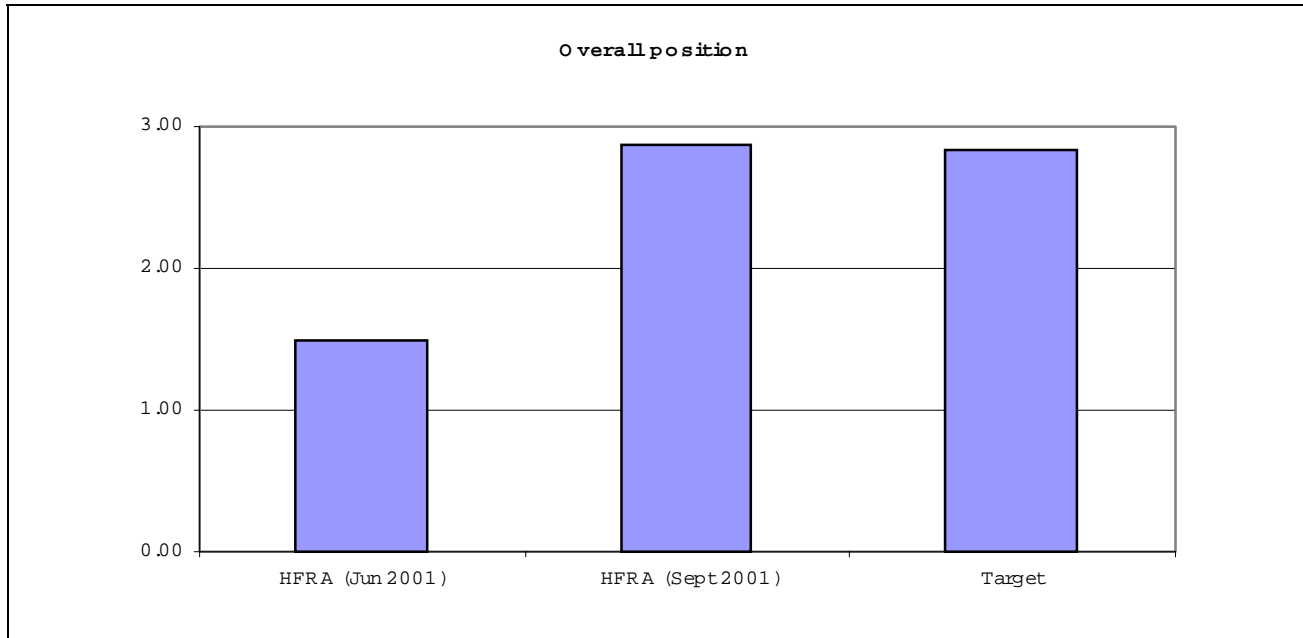
The report resulting from the first round of audit was accompanied by an action plan intended to provide a record of completion of each action during the period between the first and second rounds of audit.

## Main conclusions

The Authority's current performance is shown in Exhibit 1. This indicates a good level of preparedness when compared to the projected target.

## EXHIBIT 1 PROGRESS ON COMPLIANCE WITH THE DPA 1998

Overall, significant progress has been made since the previous audit and actions in place should ensure that overall compliance would be achieved by the October 2001 deadline



Source District Audit national database

This shows that excellent progress has been made over the last three months towards full compliance, and that the Authority has met the nationally set target. This is a position not many organisations have achieved.

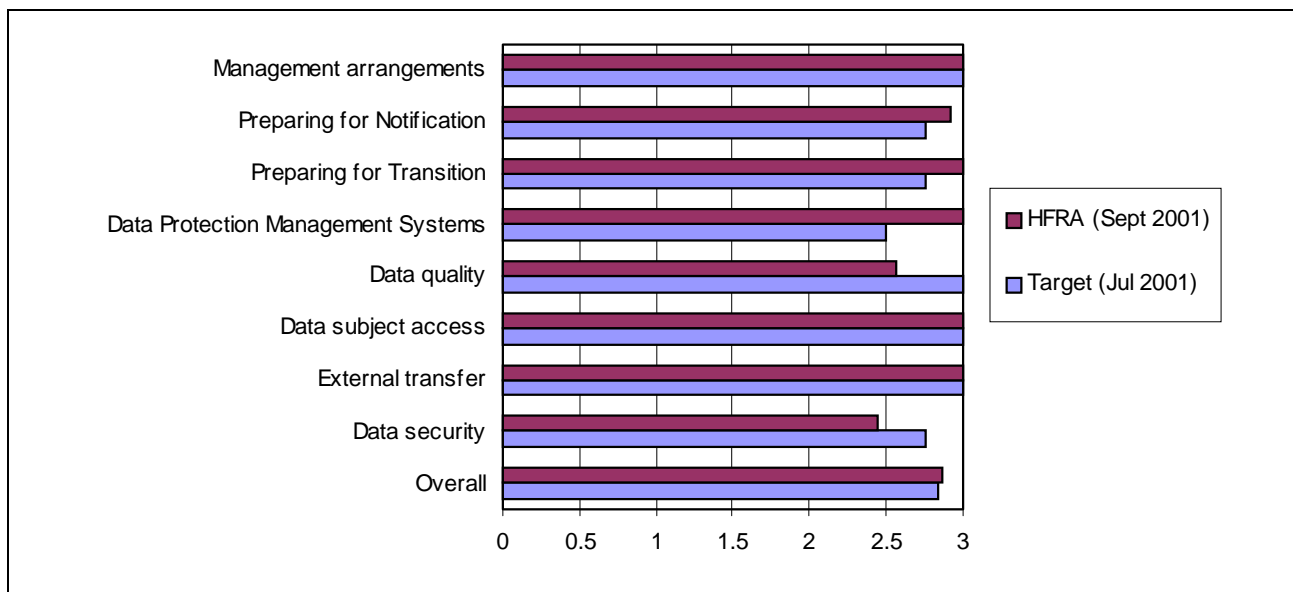
Whilst data held manually, rather than electronically, does not require Notification by 23 October 2001, the officers responsible are aiming to be able to provide assurance that it would be possible to supply a data subject with information, some of which may be stored on manual data systems, from 24 October 2001.

The Authority is therefore advised to continue to pursue the planned course of review of the relevant manual files, to identify those containing notifiable personal data.

The scoring for each of the sections of control comprising the review is shown in Exhibit 2.

## EXHIBIT 2 DETAILED SCORING OF PROGRESS AGAINST EACH OF THE DPA SECTIONS

Only two of the eight audit control areas are below the current target ie Data Quality and Data Security. These require some additional effort in order to meet the overall deadline



Responsibility for Data Protection, Human Rights and Freedom of Information Acts, may lie with different members of staff, therefore there is a need for the Authority to respond in a co-ordinated way and consequently procedures need to be put in place to ensure this.

## The way forward

The current momentum will need to be sustained if overall compliance is to be attained before the 24 October 2001 deadline.

Management needs to support the officers involved in this work by ensuring that appropriate resource levels are available to complete the tasks planned to ensure compliance and to monitor progress of this work regularly up to and beyond the first Transition deadline of 24 October 2001.

The Action Plan identifies the tasks that will need to be completed to ensure compliance with the Act's provisions by 24 October 2001. We do not intend to review the Authority's progress against this Action Plan again before the October deadline.

Whilst action has now commenced in all control areas, some work remains outstanding, particularly in addressing the following:

- update the Security Policy for Notification
- corporate standards and procedures for data receipt and entry
- a review of audit procedures for maintaining data accuracy eg third parties
- inclusion of access control reviews for systems containing notified data within the Audit Plan
- review and independent testing of back-up and recovery plans and procedures and business continuity plans and procedures
- assurance that non-magnetic/digital media are disposed of in a secure manner.

## Acknowledgement

We would like to thank the officers of Hampshire Fire and Rescue Authority for their assistance in the completion of this review.

Action point	Section ref	Action	Started	Completed	Priority	Comments
<b>1 Management arrangements</b>						
1	1.1/1.2	Identify/appoint a Chief Officer to lead on DP and progress DPA work.	●	●		
2	1.3	Ensure Data Protection Officer (DPO) is trained and has resources.	●	●		
3	1.4	Ensure that DPA and information Management on Management Team agenda.	●	●		
4	1.5	Project team of departmental officers with high level sponsor.	●	●		
5	1.6	DP Policy is in place, which covers 1998 Act.	●	●		
<b>2 Preparing for Notification</b>						
6	2.1	Timetable of expiry of current registrations, and way forward.	●	●		
7	2.2	Review accuracy of existing registrations.	●	●		
8	2.3	Reduce register entries to one Notification.	●	●		
9	2.4	Audit of all manual filing systems.	●	●		
10	2.5	Update the Security Policy for notification.	●	○	●●●	
11	2.6	Identify any additional purposes for notification.	●	●		
<b>3 Preparing for Transition</b>						
12	3.2	Prepare an action plan for transition.	●	●		
13	3.3	Identify 'new processing' (ie from 24.10.1998).	●	●		
14	3.4	Develop project control for the data audit and corporate database.	●	●		
15	3.5	Schedule of personal data, identifies which condition is being relied upon to allow processing.	●	●		
16	3.6	Identify data subject to certain exemptions within the Act.	●	●		
17	3.7	Policy on consent, identify forms in all departments requiring implicit consent.	●	●		

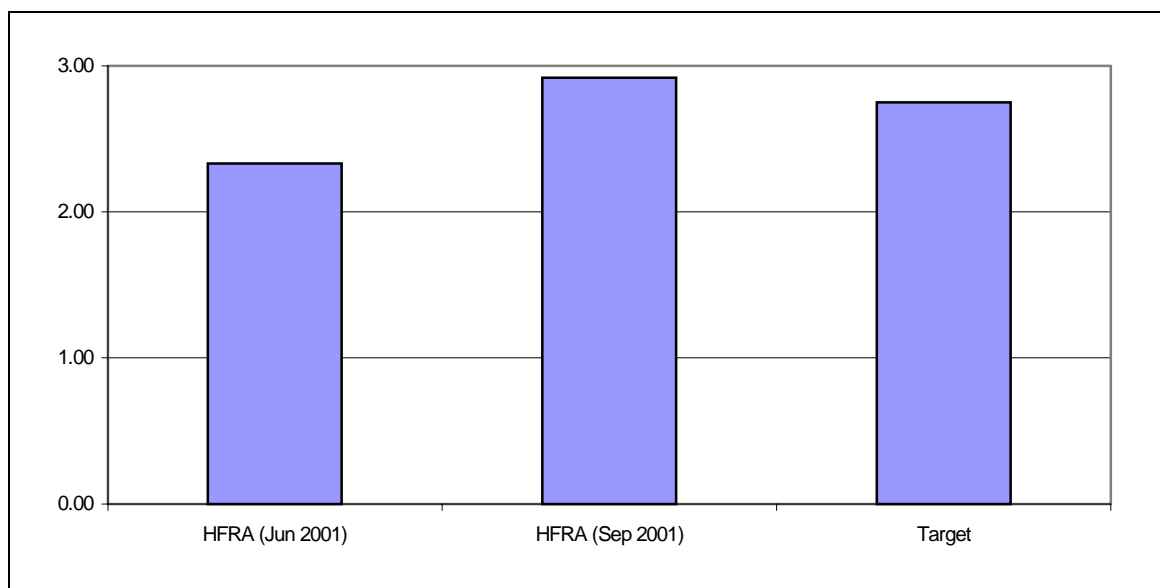
Action point	Section ref	Action	Started	Completed	Priority	Comments
<b>4 Data Protection Management System</b>						
18	4.1	Ensure all purposes to be notified can be linked to all relevant departmental data sets and include in corporate database.	●	●		
19	4.2	Identify procedures needed by staff to deal with sensitive personal data.	●	●		
20	4.4	DPO informed of proposed new or changes to systems. Incorporate in change control procedures.	●	●		
21	4.5	Monitoring system should identify to whom departments disclosure data.	●	●		
22	4.6	System should identify changes of data or its change of use and incorporate in change control procedures.	●	●		
23	4.9	Develop data classification and publication policies.	●	●		
<b>5 Data quality</b>						
24	5.1	Develop policy on checking accuracy of data receipt.	●	○	●●●	
25	5.2	Develop corporate guidelines for all staff on data accuracy.	●	●		
26	5.3	Develop policy on checking corporate data entry standards.	●	○	●●●	
27	5.4	Identify whether departments are able to trace who changes data within their systems	●	●		
28	5.5	Review audit procedures for maintaining data accuracy eg third parties.	●	○	●●	
29	5.6	Timetable for investigating retention dates on live and in store data.	●	●		

Action point	Section ref	Action	Started	Completed	Priority	Comments
<b>6 Data subject access procedures</b>						
30	6.1	Raise profile of DPO with front-line staff, Reception and post room.	●	●		
31	6.2	Ensure staff are aware of 40-day rule.	●	●		
32	6.3	Ensure data subject access procedures are in place and subject access forms available.	●	●		
33	6.4	Data subject access procedure tested.	●	●		
34	6.5	Guidance from DPO on disclosure to third parties and minors.	●	●		
35	6.7	Identify all data sets subject to automated decision-making and identify in corporate database.	●	●		
<b>7 External transfer of data</b>						
36	7.1	Develop a vetting procedure for the overseas transfer of data.	●	●		
37	7.2	Produce a web publishing policy.	●	●		
38	7.3	Distribute e-mail policy and guidance to staff.	●	●		
39	7.4	Ensure DPO involvement in development of all departmental data exchange protocols.	●	●		
40	7.5	Procedure for assuring compliance of external suppliers to DPA.	●	●		

Action point	Section ref	Action	Started	Completed	Priority	Comments
<b>8 Data security</b>						
41	8.1	Review personnel procedures for handling of DPA issues for all staff.	●	●		
42	8.2	Staff awareness and training in DPA issues programme.	●	●		
43	8.3	Ensure periodic audit of controls over notified data are in Internal Audit Plan.	●	○	●●●	
44	8.4	Address departmental security over manual files.	●	●		
45	8.5	Ensure DPO informed of all security breaches.	●	●		
46	8.6	Review and test Back-up and Recovery of electronic data to comply with 40-day rule.	●	●		
47	8.7	Review and test Disaster Recovery of systems processing notified data.	●	○	●●●	
48	8.8/8.9	Policies on disposal of magnetic media and paper needs to be formalised.	●	○	●●●	

## Preparing for Notification (Section 2)

Notification replaces Registration under the 1998 Act. All current registrations should be reviewed and then the Notification process completed. All non-exempt manual files also need to be included, as they will be subject to data subject access provisions. The Authority need to ensure that it has a formal security policy that fully satisfies the requirements of the Notification process.



Source District Audit national database

### Progress made to date:

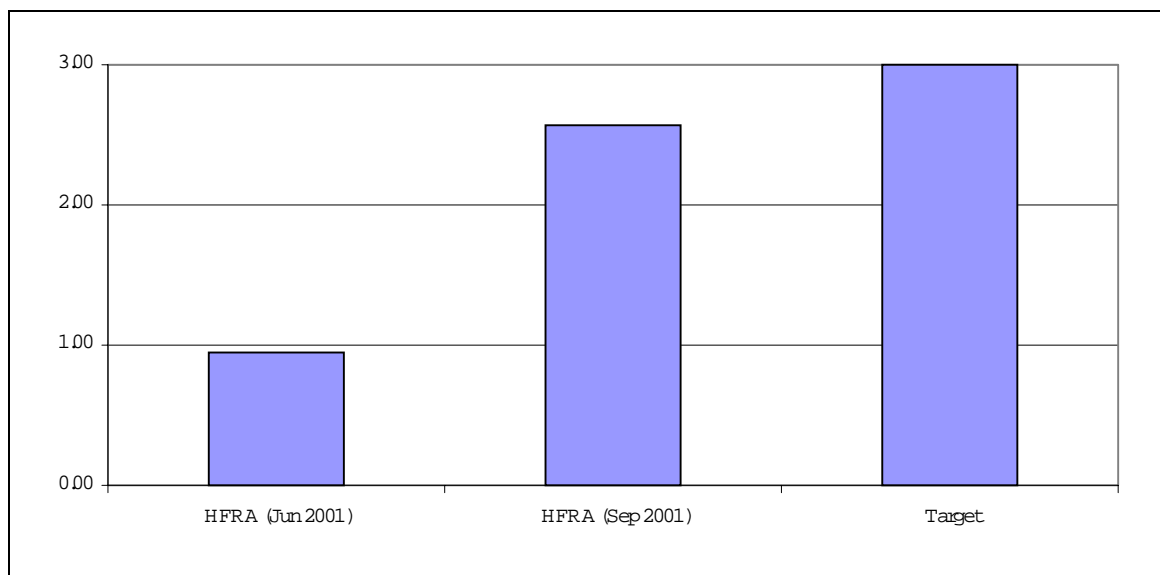
- the DPO is identifying additional purposes for Notification
- review of existing registrations complete
- timetable for notification prepared
- manual data-sets being identified
- policy for notification of manual files identified.

### Action still required:

- update the Security Policy for notification.

## Data quality (Section 5)

Principles 3, 4 and 5 of the Act impose duties on the Authority's data controllers to ensure that the data they hold is adequate, relevant, not excessive, accurate and up-to-date and kept for no longer than necessary for purposes for which it has been notified. The Authority needs to develop policies on data receipt and corporate data entry standards, and review its audit procedures for data accuracy.



Source District Audit national database

### Progress made to date:

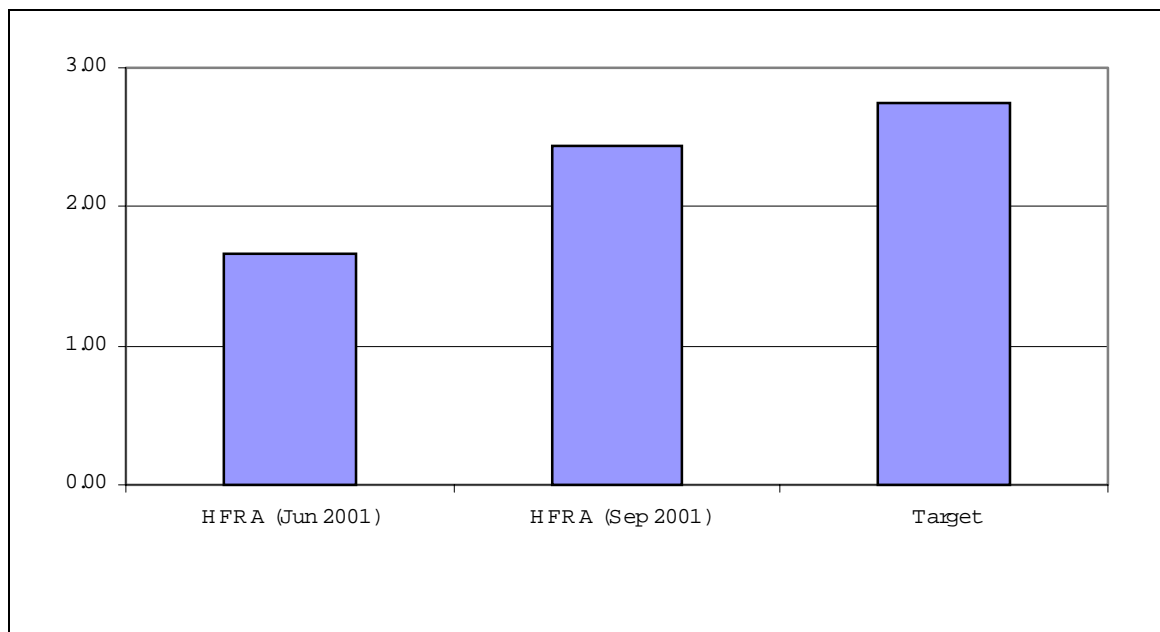
- review of data storage retention periods complete
- policies on staff responsibilities being updated
- regular data reviews raised in the Functional Data Managers group
- system to monitor changes of data in place
- requirement for data storage review part of project team responsibility.

### Action still required:

- develop policy on checking data receipt and corporate data entry standards
- review audit procedures for maintaining data accuracy eg third parties.

## Data security (Section 8)

The Notification form within the Act requires a description of the information security policy being followed by the Authority to assure data integrity and privacy. The Information Commissioner reserves the right to refuse to accept notification on grounds that could include reservations over the security of personal data and especially sensitive personnel data. The Authority needs to review its disaster recovery and business continuity plans and introduce formal policies on the disposal of magnetic and non-magnetic media.



Source District Audit national database

### Progress made to date:

- staff conditions of service being reviewed and Awareness programme underway
- review security over manual files and consider implications for security policy
- DPO informed of all security breaches.

### Action still required:

- ensure periodic audit of controls over notified data are in Internal Audit Plan
- Disaster and Recovery Plans and Business Continuity Plans to be reviewed
- policies on disposal of magnetic media and paper needs to be formalised.