

The Ombudsman's assessment of the loss of personal data by a Home Office contractor

The Ombudsman's assessment of the loss of personal data by a Home Office contractor

Fifth report

Session 2009-2010

Presented to Parliament pursuant to
Section 10(4) of the Parliamentary Commissioner Act 1967

Ordered by
The House of Commons
to be printed on
22 March 2010

HC 448
London: The Stationery Office
£9.50

© Crown Copyright 2009

The text in this document (excluding the Royal Arms and other departmental or agency logos) may be reproduced free of charge in any format or medium providing it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

For any other use of this material please contact the Office of Public Sector Information, Information Policy Team, Kew, Richmond, Surrey TW9 4DU

or e-mail: licensing@opsi.gov.uk.

ISBN: 9780102964622

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID 2354645 03/10
PHSO-0089

Printed on paper containing 75% recycled fibre content minimum.

Contents

Foreword.....	5
Introduction	7
The complaints	9
The information contained on the data stick	9
The events that led to the complaints.....	11
How the data loss happened	11
The Home Office’s position on the information contained on the data stick.....	11
The Home Office’s communication strategy	12
Risk Assessments	13
The external scrutiny report.....	14
The Information Commissioner’s decision not to take enforcement action	14
Claims for compensation.....	14
The Prisons and Probation Ombudsman.....	15
The reasons for my decision	16
The assessment process	16
Principles of Good Administration.....	16
Consideration of maladministration.....	17
Consideration of injustice	20
Conclusion.....	22

Foreword

I am laying this report before Parliament under section 10(4) of the Parliamentary Commissioner Act 1967.

Over a period of four months last year I received 449 individual complaints from prisoners and former prisoners about the loss by the Home Office of sensitive personal data about them on an unencrypted data stick. Over 240 Members of Parliament have referred those complaints to me, and this report explains why I have decided not to investigate them.

In August 2008, a contractor working for the Home Office lost the data stick containing personal data of at least 84,000 prisoners, including names, addresses and some offence codes. The complainants have expressed their shock and anxiety about the data loss and said that this was compounded by a lack of helpful information provided by the authorities. They have asked for a compensation payment for the fear, inconvenience and risk to their own and their families' safety that they say has occurred.

In this report I explain my approach to assessing complaints and deciding whether I could and should investigate them. One aspect of my approach is to assess whether there is some evidence of maladministration. I have seen clear indications of maladministration surrounding the circumstances leading to the loss of the data by the Home Office. However, I have not seen any indication of maladministration in the way the Home Office responded to the data loss.

If I see indications of maladministration, I assess whether there is unremedied injustice as a consequence of that. Much of the information that was on the data stick is already in the public domain. It seemed to me, therefore, that complainants could not reasonably claim to be

worried about its contents being made public and I find it difficult to see any merit in a compensation claim for additional anxiety resulting from the loss. Moreover, the Permanent Secretary of the Home Office has asked me to pass on his apologies for this loss of data and for any loss of public confidence in the security of Home Office systems that contain personal data. The contractor has publicly apologised. Overall, therefore, I am not persuaded that there is unremedied injustice as a consequence of the loss of the data stick.

My report highlights the need for public bodies to consider proactive and timely communication with individuals if their data has been lost, particularly in advance of likely media reporting. In the case considered here, the Home Office decided not to contact the majority of those affected in advance, but to let them learn about the loss through press reporting. It is clear that those who complained to me do not feel that they received sufficient information or reassurance. A different, more proactive, approach might have avoided these complaints coming to my Office.

I know that part of the reason the complainants are concerned about the data loss is because they do not feel that they have been fully briefed on the information contained on the data stick. However, the Home Office have set up arrangements to ensure that any individual who considers that his or her data may have been lost as a consequence of the loss of the data stick will receive a written response from the Home Office setting out the data fields in which the individual may have been included. The solicitors representing the vast majority of the complainants were given information in April last year and the information I provide in this report should go some way to ease the complainants' outstanding concerns. As I have said, I have not seen any indication of

maladministration in the way the Home Office responded to the data loss.

This incident of data loss has already received significant public attention, both at the time of the loss and in the months since. Many MPs have been involved in referring complaints to me. While it is unusual for me to lay a report before Parliament outlining my decision not to investigate complaints, I hope that this report will provide a detailed response to those MPs who have represented the complainants, and place on the record my reasons for not investigating on this occasion.

A handwritten signature in black ink that reads "Ann Abraham". The signature is written in a cursive, flowing style.

Ann Abraham
Parliamentary and Health Service Ombudsman

March 2010

Introduction

- 1 Between 10 July and 12 November 2009 I received 473 individual complaints about the loss of an unencrypted data stick by a contractor working for the Home Office. Of these, 24 complaints were not referred to me by an MP and as such were closed as not properly made. That left 449 complaints for me to consider. Given that all of these 449 complaints were essentially about the same issue, the loss of the data stick, I have looked in detail at the events as they affected the complainant in one lead complaint, which I am satisfied is representative of the complaints put to me. This report explains why I have decided not to investigate these complaints.
- 2 In the course of my assessment of these complaints I have considered the complaint that was put to me by the lead complainant and I have received further information from the solicitors who represent the vast majority of complainants. In addition, I have made enquiries of the Home Office and have received information from them direct. That information included a letter from the Permanent Secretary of 13 November 2009, which provided additional information about the work that had been undertaken in assessing the risk to individuals caused by the data loss.

The complaints

- 3 The complainants are concerned that the Home Office has lost an unencrypted data stick containing sensitive information about them. They believe that the data stick contains highly sensitive information about them and that, if it were to get into the wrong hands, it could leave them and their families open to retribution from various sources, including their victims and vigilante groups.
- 4 Most of the complainants have used a standard template to present their complaints to me and therefore much of the detail of the complaints is similar, albeit they have been slightly personalised. The following areas of concern are representative of the complaints put to me:
 - worry and shock about the data loss, and for many this seems to be compounded by a lack of helpful information given to them by the relevant authorities;
 - increased anxiety levels and increased stress, which has led to disturbed sleep; many complainants have mentioned not being able to sleep or having nightmares and some have mentioned seeking medical assistance with this; and
 - feeling that this situation means that their conviction will stay with them forever; some complainants have commented that it will affect their job prospects.
- 5 The complainants are seeking a compensation payment for what they describe as the fear, inconvenience and risk to their own and their families' safety caused by the data loss. It is not specified how much they are seeking in terms of

compensation but it is clear that the majority of complainants believe a compensation payment would be appropriate.

The information contained on the data stick

- 6 Before turning to the events giving rise to the complaints, I consider that it would be helpful to clarify at the outset the information I understand is contained on the missing data stick. There seems to be a lack of certainty about the information that is contained on the missing data stick, but the Association of Chief Police Officers' confidential briefing note on the data loss provides more detailed clarification than I have seen elsewhere. It seems to me to be the most comprehensive assessment of the missing data and I have used this to inform my decision. The Association of Chief Police Officers estimated that the missing data included:
 - approximately 33,000 Police National Computer (PNC) nominal records containing details of names, dates of birth, addresses and PNC identification numbers;
 - information on the whole of the prison population of 84,000 subjects, detailing names, dates of birth and in some cases expected prison release dates and Home Detention Curfew Data;
 - 10,000 details of Prolific and Priority Offenders¹ containing the names, dates of birth and PNC identification numbers; and

¹ Prolific and Priority Offenders (PPOs) are essentially those offenders who have been identified as committing the most crime and causing the most harm to their communities. The PPO programme provides a joined up, multi-agency offender management model involving representatives from the local police and probation services, local authorities and youth offending teams. The three strands of the programme are: deter, catch and convict, and rehabilitate and settle.

- Drug Intervention Programme data, with approximately 10,000 offenders' initials, PNC ID numbers and other associated information, including offence details. The offence details were provided as offence codes and so it would take an understanding of the criminal justice system to interpret the relevant codes.
- 7 If the Association of Chief Police Officers' description of the missing data is correct, then it is possible that somewhere between 84,000 (assuming complete overlap) and 137,000 (assuming there is no overlap) people have been affected by the loss. This is clearly significant.

The events that led to the complaints

How the data loss happened

- 8 On 18 August 2008 an employee of a Home Office contractor lost a memory stick containing information about offenders, some of whom, but not all, are still in prison. The contractor had been contracted to administer the JTrack² system for the Prolific and Priority Offender programme. The contractor warned the Home Office of a possible loss late on 18 August and this was confirmed on 19 August. The Home Office notified the Information Commissioner about the loss during a telephone conversation on 21 August and provided formal notification to the Information Commissioner, in the form of a report, on 10 September. The loss was reported extensively in the media on 22 August.
- 9 In their notification report of 10 September 2008 to the Information Commissioner, the Home Office said that there were 10,000 to 11,000 prolific and priority offenders being actively managed in England and Wales. They explained that the contractor provided the JTrack hardware, software and system support under contract to them and that the contractor regularly received information from the Home Office and the National Policing Improvement Agency. The Home Office said they were satisfied that all information transferred by them was appropriately secure but that an employee of the contractor transferred data on to an unencrypted memory stick in breach of the contractor's own security policy.
- 10 It seems that the contractor's employee received (via secure email from the Home Office) two data sets – Prisoner data and Prolific Offender data – and downloaded them in a non-secure area and transferred them on to an unencrypted memory stick. The employee then received a third data set from the National Policing Improvement Agency by way of encrypted CD ROMs and transferred it again to the same memory stick in a non-secure area of the office. As part of a separate process, a fourth dataset was downloaded directly from the JTrack system to the same memory stick in order to send this information by way of secure email to another contractor involved with processing Drug Intervention Programme data. The Home Office told the Information Commissioner that they were satisfied that the contractor had breached their contract with them and so they had terminated it. They explained that they are now supporting the JTrack system in-house.

The Home Office's position on the information contained on the data stick

- 11 In their notification to the Information Commissioner, the Home Office also explained that it was not possible to confirm categorically the extent of the information on the missing memory stick. They estimated (based on the recollections of the contractor, their regular processes and knowledge of what was sent to the contractor by the Home Office or National

² JTrack is a Home Office system and it is an operational tool used by the Police and the Crown Prosecution Service to support the Government's Prolific and other Priority Offender (PPO) programme. The custody details of PPOs have been entered on to the JTrack system since 2006. The purpose of the system is for individual areas to see when one of their PPOs enters custody, is moved between prisons, and is due for release and from which establishment. The Home Office have said that this is a useful tool for reducing crime and it ensures that prolific offenders are not released in to the community without the knowledge of the local police, who I understand often meet prisoners as they leave prison. The Police National Computer is used to provide the information on persistent offenders.

Policing Improvement Agency) that the memory stick contained:

- data from the Police National Computer, including the personal details of individuals with six or more recordable convictions in the preceding 12 months;
 - names of prisoners in custody in England and Wales with prisoner and prison identity codes, expected release dates and Home Detention Curfew dates in some cases;
 - details of prolific and priority offenders; and
 - details of individuals on Drug Intervention Programmes.
- 12 That concurs with the information that the Permanent Secretary to the Home Office gave me in his letter of 13 November 2009. He also pointed out that there would be some overlap between the data sets as some prolific and priority offenders would be included in the list of those in custody. He said that he could not determine with sufficient precision the extent to which the data sets overlapped in order to provide a figure for the total number of individuals concerned. However, given the further research that the Association of Chief Police Officers have undertaken on the contents of the data stick and the numbers affected, which I have set out above, it seems to me that a more accurate description of the position is that it would take more extensive analysis to be more precise about the overall numbers and that would not be proportionate at this stage. As I have explained above, I have relied on the Association of Chief Police Officers' more detailed description of the information contained on the data stick and the numbers affected.

The Home Office's communication strategy

- 13 The Home Office have told me that following the loss, a Steering Group, which included representatives from the Association of Chief Police Officers, the Home Office, the Ministry of Justice, the National Policing Improvement Agency and the Metropolitan Police (and in discussion with the Information Commissioner), decided not to contact everyone who might be affected by the data loss. The Permanent Secretary has told me that this was because many of them were either active or former offenders and the police were aware that many of them might be difficult to locate. They considered that communicating through a third party might cause more worry and distress, as they could not be sure whether family and friends were aware of the details of the individual's convictions, and giving them information about an individual's conviction might actually cause more distress to that individual.
- 14 In their notification to the Information Commissioner of 10 September 2008, however, the Home Office said that they considered that the disadvantages of contacting those affected outweighed the benefits of doing so, and that it would probably exacerbate the situation rather than help. They said that they had reached that decision because:
- communication to the prison population was being managed by prison governors, which would minimise the risk of disruption within prisons;
 - addresses given by individuals in the criminal justice system can often be unreliable and there was a high risk of giving away sensitive

data about criminal records by writing to incorrect addresses;

- support was available to those affected via the public enquiry contact points; and
 - the risk to the vast majority of individuals had been assessed as low and contingency plans had been put in place to respond quickly in the unlikely event of the data becoming public.
- 15 Whatever the precise rationale, the Home Office have told me that the Ministry of Justice sent a notice to chief probation officers and prison governors with a brief outline of the missing data; the intention was that this would enable them to respond to any concerns raised by prisoners or those under probation supervision. The assumption was that those affected would find out through the media and relatives and, if they had any concerns, these could be addressed by the prison governors or probation officers who had already been briefed. The Home Office's general enquiry line was also briefed to deal with any calls on the subject.
- 16 The Home Office have also told me they have set up arrangements to ensure that any individual who considers his or her data may have been lost as a consequence of the loss of the data stick, will (upon proof of identity) receive a written response from the Home Office setting out the data fields in which the individual may have been included. In many instances, individuals' details will have appeared on more than one of the data sets, requiring an individual response in each case. So far, the Home Office have provided this information to more than 800 individuals.

Risk Assessments

- 17 As I have touched on above, the Home Office did, however, take action to consider the risks of the data being made public, and the Association of Chief Police Officers drew up a risk assessment with mitigation in terms of the most at risk groups. They identified that the most at risk groups would be sex offenders and witnesses on protection if they were affected. Witnesses were not affected by this loss and so sex offenders were considered to be the most at risk group. They considered those at risk in this group were the people whose names, addresses and offence details could be matched. They identified 34 sex offenders in this group, of whom three were of no fixed abode, ten were out of prison and 21 were still in prison. In these cases the relevant local police force was notified to consider any risks the loss posed to the offenders' families, with any decision to contact the individual or family made locally. That was in line with the risk assessment, which said that:

'Relevant police forces will be informed of the details of the sex offenders who have been identified as potentially at risk and are currently not within prison. Details will be passed to the MAPPA [Multi Agency Public Protection Arrangement] teams in order that crime prevention advice can be provided to the individuals where appropriate. In doing so, this will enable the most recent information available to be considered as part of the process.'

- 18 The risk assessment went on to say that prison authorities were handling notification to individuals currently within their establishments and Multi Agency Public Protection Arrangement teams would be notified of any imminent release dates. The

Permanent Secretary has told me that as of 13 November 2009, a total of eleven individuals were visited personally by the police and prison staff and a further seven were informed through their families, where there was confidence that the family was in close contact with the individual. (I do not know why the 13 other people potentially at risk, and whose whereabouts were known, were not contacted but I do not believe that this is material to my assessment which follows.)

- 19 The Association of Chief Police Officers also considered that there was a low to medium risk of those affected being subject to fraudulent crime. That was because the data stick did not contain financial information about individuals. That was to be mitigated by the provision of advice to anyone concerned on how to be vigilant in respect of their finances.

The external scrutiny report

- 20 The Home Office also commissioned an external scrutiny report to look into the way they had handled matters. The report was completed in late September 2008 and concluded that the Home Office had responded appropriately and well to the incident; appropriate risk assessments had been conducted to assess the possible implications for individuals and steps taken to mitigate such risks. The report also noted that the Home Office had identified important lessons from the incident, particularly the urgent need to improve controls and audits of their commercial suppliers. The report also made a number of recommendations for further action in relation to embedding the learning from this incident and preparing a good practice guide for senior managers.

The Information Commissioner's decision not to take enforcement action

- 21 The Information Commissioner decided not to investigate the data loss as the Home Office had notified him appropriately, promptly investigated and on 10 September 2008 provided formal notification in the form of a report (which was independently scrutinised later that month). The Information Commissioner decided that enforcement action was not required as the Permanent Secretary had signed an undertaking to ensure that data are processed in accordance with the *Data Protection Act* and that the Home Office would check its data processors for compliance with that; and because the Home Office had taken the matter seriously.

Claims for compensation

- 22 On 29 March 2009, the solicitors who represent a large number of the people who have complained to me wrote separately to both the Home Office and to the Home Office contractor saying that they had been instructed by over 1,000 prisoners in connection with the data that went missing in August 2008. They maintained that the Home Office/the contractor had not complied with the *Data Protection Act* and that they intended making a formal complaint to the Information Commissioner. Before doing so, they asked the Home Office/the contractor to provide copies of any reports and full details of subsequent action taken; to state the date and circumstances of the loss and what information was lost.
- 23 The Home Office replied on 22 April 2009 enclosing copies of their internal report

of 10 September 2008 to the Information Commissioner and the external scrutiny report. They said the reports answered all of the solicitors' questions. They invited them to contact them if they required any further information.

- 24 In response to claims for compensation the Home Office have received direct, they have provided a generic response, which explains that they consider there are no grounds to uphold a complaint or seek compensation as the risk assessment had determined that there was no heightened risk to individuals or their families. That was because the data did not include any financial information and all the individuals concerned had Police National Computer identification numbers, meaning that data relating to them were already in the public domain.

The Prisons and Probation Ombudsman

- 25 I understand that the solicitors have also complained to the Prisons and Probation Ombudsman about these matters, and in response he has explained that he cannot consider the complaints, as they do not fall within his remit. That is because the data was not lost by a member of staff of HM Prison Service, UK Border Agency or the National Probation Service.

The reasons for my decision

The assessment process

26 Generally when assessing complaints I first establish that a complaint falls within my remit and is therefore one I could investigate. I am satisfied that these complaints do. I then consider whether it is a complaint that I should investigate. In order to do that, I assess whether there is some evidence of maladministration on the part of the body complained about that has led to an unremedied injustice to the aggrieved person. If there is, I also want to be satisfied that an investigation is likely to result in a worthwhile outcome. My consideration of a worthwhile outcome goes wider than deciding whether an investigation could achieve an outcome that the complainant would be happy with. I also consider whether there might be a wider public interest as a result of an Ombudsman's investigation, for example, whether the learning from the complaint could be used to drive improvements in public services or inform public policy.

27 In assessing these complaints I have considered both the matters that gave rise to them and also how the Home Office responded to the situation. I have based my assessment on my *Principles of Good Administration*.³

Principles of Good Administration

28 I have taken particular account of the following Principles:

- **Getting it right:**

which includes taking proper account of established good practice – in this case the Information Commissioner's guidance on data security breach management.

- **Being open and accountable:**

which includes handling information properly and appropriately, and which also says that public administration should be transparent and that information should be handled as openly as the law allows; and that public bodies should give people information and, if appropriate, advice that is clear, accurate, complete, relevant and timely.

- **Being customer focused:**

which includes communicating effectively, using clear language that people can understand and that is appropriate to them and their circumstances, and which also says that public bodies should deal with people helpfully, promptly and sensitively, bearing in mind their individual circumstances.

³ The Ombudsman's Principles trilogy, the *Principles of Good Administration*, *Principles of Good Complaint Handling*, and *Principles for Remedy* and were published in 2007 and are based on the 40 years of experience the Ombudsman's Office has in dealing with complaints. There are six Principles in all: Getting it right, Being customer focused, Being open and accountable, Acting fairly and proportionately, Putting things right and Seeking continuous improvement. More information about the Principles can be obtained from www.ombudsman.org.uk

- **Putting things right:**

which includes acknowledging mistakes and apologising where appropriate.

Consideration of maladministration

29 There are clear indications of maladministration here in that an employee of a Home Office contractor was able to download information in a non-secure area of the office on to an unencrypted memory stick. The data stick was then lost and the Home Office are now in a position where they cannot say categorically what information was contained on the data stick. In line with the Principle of *'Being open and accountable'* outlined above, I would expect all Government departments, including the Home Office, to handle information properly and appropriately and to ensure that their contractors do so with the security of data kept in mind at all times. That could involve, for example, regular checking on compliance with the security arrangements. While it was not the Home Office who lost the data but an employee of one of their contractors, as they are the body responsible for the proper handling of the data, it is their responsibility to ensure its safety. That did not happen here.

30 However, it is clear that following the data loss, the Home Office took a number of positive measures in order to put matters right. I have referred above to the Information Commissioner's guidance on data security breach management. In line with the Principle of *'Getting it right'* outlined above, I have considered whether the Home Office response to the data loss took adequate and appropriate account of the four important elements the Information Commissioner advises should be

included in any data breach management plan. Those are:

- Containment and recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response.

31 In terms of containment and recovery, the Home Office took prompt action to investigate the breach and provided a report for the Information Commissioner on the breach on 10 September 2008. The Home Office concluded, after investigation, that it was likely that the data stick was stolen by an opportunistic thief for its intrinsic value and not because of the data it contained. That all seems to me to be reasonable.

32 In terms of ongoing risk assessment, the Home Office acted quickly to convene a Steering Group to consider the data loss, to consider the risks to individuals affected and to consider the communication plan. That is in line with the Information Commissioner's guidance on assessing ongoing risks. I will say more about the communication plan below.

33 The Home Office's overall approach to risk assessment following the data loss seems to me to be reasonable, especially in terms of the risk assessments undertaken by the Association of Chief Police Officers. They identified that it was sex offenders, whose addresses might be matched to their crimes (albeit it would require a knowledge of offence codes to make the match), who were most at risk from harm. In line with the risk assessments, 34 individuals were identified in this high risk category and

- the relevant local bodies were made aware of this and given the task of communicating to the individuals concerned and ensuring plans would be put in place if the information were ever made public. Multi Agency Public Protection Arrangement teams were also notified of release dates of those in this high risk group. It seems to me to be sensible for the Home Office to have relied on local bodies, such as the police, prison governors and probation officers, to make decisions about communications with people within this group and a reasonable way of dealing with the risk that had been identified.
- 34 The Home Office also considered the risk of the information contained on the data stick being used for the purposes of fraudulent crime. They considered that that risk was low to medium, given that none of the datasets contained financial information. The risk assessment considered that the risk could be mitigated by the provision of advice on how to be vigilant about finances. That also seems to me to be reasonable.
- 35 I turn next to evaluation and response. I note that the Home Office commissioned an external scrutiny report to look at the way the situation had been handled, and lessons that had been learnt from that. In addition, because the action of the contractor's employee was a clear breach of both the contract the Home Office had with the contractor, and also with the contractor's own internal procedures, the Home Office swiftly terminated the contract with the contractor and have brought the administration of the JTrack system in-house. These actions all seem to me to represent positive measures that demonstrate that the Home Office sought to learn from this incident and to ensure that it does not recur.
- 36 That leaves the issue of notification. There is no doubt that the Home Office acted promptly to notify the Information Commissioner about the loss and later gave formal notification in the form of the report of 10 September 2008. The work with the Information Commissioner resulted in the Home Office signing an undertaking that they would take steps to ensure that all processing done by a data processor would be done in line with the security measures governing that and that they would carry out regular inspections to ensure compliance.
- 37 There is, of course, another side to providing relevant notification and that is the question of whether, and if so how, to communicate the fact of the data loss to those affected.
- 38 The Home Office was aware that the matter was going to be reported extensively in the press on 22 August 2008, but decided that they would not be proactive in terms of letting those affected know about it. Rather, they took the decision to let those affected learn of the loss through the media, with the onus then being placed on those individuals to contact the relevant authorities (prison governors, probation officers or the general enquiry line) for further information and clarification if they felt they needed it. The Home Office had ensured by way of the Steering Group that prison governors, probation officers and enquiry line staff had been briefed so that they could deal with any questions put to them.
- 39 The Home Office's communication strategy was clear but was it reasonable? I have considered whether there are any indications of maladministration in what the Home Office did – and did not – do in relation to communicating

- with the individuals affected by the data loss. It was, after all, their data.
- 40 After considerable reflection I have decided that I cannot say that the Home Office's communication strategy was unreasonable. First, the Home Office acted correctly in that they considered whether or not it was appropriate to notify the individuals concerned about the data loss. I accept that the Home Office and members of the Steering Group are more familiar than I am with the difficulties of communicating with the offender and ex-offender population. I recognise that those difficulties were likely to have been a relevant consideration in their decision; and I cannot say that the decision to brief prison governors, probation officers and the enquiry line with the information they needed to respond to enquiries once the fact of the data loss became public was an unreasonable way of dealing with the situation.
- 41 Notwithstanding that, it seems to me that the communication strategy might usefully have drawn more clearly than it did on the Ombudsman's Principles of '*Being open and accountable*' and '*Being customer focused*'. If it had done, it seems to me that the Home Office might have decided to give the individuals affected information about the data loss directly and sooner and might have done so in a more helpful and sensitive manner.
- 42 As I see it, when a public body has lost personal data, normally the public body should be proactive and open in their communications with those affected about the data loss, rather than place the onus on those affected to seek out the information, **unless there are good reasons not to adopt this approach.**
- 43 There might be good reasons not to adopt this approach, for example, if the public body has assessed that there is a very low likelihood of the data itself, and/or the fact of its loss, coming into the public domain. In such circumstances, notification to those affected might well cause worry and distress needlessly.
- 44 However, in this case, the Home Office knew that the data loss was going to be reported in the media, and when that was likely to happen. It was highly likely therefore that worry and distress **would be** caused to those affected. In those circumstances it seems to me that it would have been better for arrangements to have been put in place to ensure that some form of proactive communication was issued with the aim of minimising the extent of that worry and distress.
- 45 I am not suggesting that the Home Office should have written personally to each person who was affected. I understand that they decided not to do so because of the difficulties involved in communicating with the offender population and the associated risks of notifying family members or friends who might not be aware of all the details of the offender's conviction. However, as the entire prison population was affected by the data loss, a communication could have been issued to prison governors to pass on in an appropriate way. The Home Office did, after all, have something of a captive audience. Similarly, probation officers could have been given the same communication to pass on to those on probation. In that way those affected would have been provided with timely, relevant and complete information at the outset, rather than having to seek it out for themselves, once they had found out about the loss from the media.

46 Moreover, the Home Office, with the Steering Group, had put a lot of thought and effort into establishing the nature and extent of the data loss and considering the risks to individuals, which meant that there were a number of positive messages they could have given to those affected. For example, they knew that the data stick contained only limited information and had assessed that only 34 individuals were at high risk.

47 It is clear that those who complained to me do not feel that they received sufficient information or reassurances from the relevant authorities. A general communication could have been helpful in ensuring that those affected received the same information and advice. Such a communication could have given details of the information that was contained on the data stick, explained where those affected could go for further information and advice and outlined the steps that were being taken to contact separately the 34 individuals considered to be in the high risk group. That information could have provided considerable reassurance to those affected and mitigated the extent of worry and distress caused.

48 I am not suggesting that the Home Office's failure to adopt the approach and take the sort of steps that I have outlined above amounts to an indication of maladministration. As I have already said, I have concluded that I cannot describe the Home Office's communication strategy as unreasonable. But I do think it could have been better, and that if the Home Office had adopted a different, more proactive, approach, these complaints might have been avoided.

Consideration of injustice

49 I turn now to my assessment of whether there is any evidence of unremedied injustice as a result of the alleged maladministration.

50 In these cases the complainants are seeking compensation for what they have described as the fear, inconvenience and risk to their own and their family's safety caused by the data loss. It seems that at the heart of their anxiety is the lack of information they received up front about the information contained on the data stick. In response to the compensation requests, the Home Office have explained that the Association of Chief Police Officers had determined that there were no heightened risks to individuals or members of their families as a result of the loss of the data stick because the lost data did not include any financial information about them, and all the individuals involved had PNC identification numbers, which meant that data relating to them was already in the public domain. On that basis the Home Office decided that a compensation payment would not be appropriate.

51 I recognise that the complainants are likely to remain of the view that a compensation payment would be appropriate but I do not agree. It seems to me that the Home Office was clearly at fault in relation to the loss of the data stick but the steps they took to consider the consequences of that and to put a communication plan in place were reasonable. In reaching that decision I am also mindful that the information contained on the data stick was largely in the public domain in any event (names, addresses and offence details) and so I cannot see any basis on which the complainants could reasonably claim to be additionally worried about its contents being made public.

In addition, in a number of cases we have found information about the complainants and their convictions readily available on the Internet. In those circumstances, it is even more difficult to see any merit in a compensation claim for the additional anxiety the complainants say they are experiencing as a result of the loss of the data stick.

publicly apologised for the data loss. Given that I do not consider that compensation would be appropriate, I am satisfied that represents a suitable remedy to these complaints.

52 Of course, I fully recognise that part of the reason the complainants are concerned about the data loss is because they do not feel that they have been fully briefed on the information contained on the data stick. However, I see that the solicitors representing the vast majority of the complainants were provided with this information in April last year and I trust that the information I have provided in this report will go some way to ease their outstanding concerns. The Home Office have set up arrangements to ensure that any individual who considers that his or her data may have been lost as a consequence of the loss of the data stick will receive a written response from the Home Office setting out the data fields in which the individual may have been included.

53 That said, I have seen no evidence that the Home Office have considered whether a remedy, other than compensation, would be appropriate. In line with the Principle of '*Putting things right*', I expect public bodies to acknowledge mistakes and apologise where it is appropriate to do so. It is clear that data should not have been lost and it seems to me that it would be appropriate for the Home Office to apologise to those affected about that. I put that to the Permanent Secretary and he has asked me to pass on his apologies for this loss of data and for any loss of public confidence in the security of Home Office systems that contain personal data. The contractor has

Conclusion

- 54 In assessing these complaints I have considered not only the matters that initially gave rise to them but also how the Home Office responded to the situation.
- 55 I have seen clear indications of maladministration on the part of the Home Office, in that data was not handled appropriately by one of its data processors. Whilst I think that the Home Office's communication strategy could have been better, overall I have not seen any indication of maladministration in the way that the Home Office responded to the situation.
- 56 The question that then remains for me is whether there is any evidence of unremedied injustice in consequence of maladministration that would lead me to investigate these cases. For the reasons set out in paragraphs 49 to 53 above I am satisfied that there is not.



Ann Abraham
Parliamentary and Health Service Ombudsman

March 2010

**Parliamentary and
Health Service Ombudsman**

Millbank Tower
Millbank
London SW1P 4QP

Tel: 0345 015 4033
Fax: 0300 061 4000
Email: phso.enquiries@ombudsman.org.uk

www.ombudsman.org.uk



information & publishing solutions

Published by TSO (The Stationery Office) and available from:

Online

www.tsoshop.co.uk

Mail, Telephone Fax & E-Mail

TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Parliamentary Bookshop

12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: <http://www.bookshop.parliament.uk>

TSO@Blackwell and other Accredited Agents

Customers can also order publications from

TSO Ireland
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401

ISBN 978-0-10-296462-2



9 780102 964622