THE DRIVING STANDARDS AGENCY DATA PROTECTION POLICY

Title:	Data Protection Policy
Classification:	NOT PROTECTIVELY MARKED
Descriptor:	Policy
Policy Reference:	POL/46/08
Summary:	Policy on how the Driving Standards Agency (DSA) processes personal data in compliance with legislation and relevant guidance
Status:	Review
Version No:	2.0.0
Date Approved:	22 July 2010
Date of Review:	June/July 2010
Policy Owner:	Head of Information Assurance
Who to contact for queries:	DSA Knowledge & Information Management Team
Related Policies and Guidance	• DSA Information Risk Policy • DSA Information Security Policy • DSA Data Sharing Policy • DSA Incident Management Policy • DSA Records Management Policy • IT and Communications Policy • DSA Information Charter • Standard Operating Procedures • Data Protection Awareness Training • IAO Packs • DSA Protective Marking Policy
Audience:	All DSA staff and authorised users of DSA systems, including temporary staff and contractors processing personal data on behalf of DSA.
Reference:	• DSA Information Risk Policy • DSA Information Security Policy • DSA Data Sharing Policy • DSA Incident Management Policy • DSA Records Management Policy • IT and Communications Policy • DSA Information Charter • Standard Operating Procedures • Data Protection Awareness Training • IAO Packs • DSA Protective Marking Policy

Policy Owner: Head of Information Assurance

Contacts: Knowledge & Information Management Team

Email: Knowledge.InformationManagement@dsa.gsi.gov.uk

Phone: 0115 936 6767

CONTENTS

1. INTRODUCTION

1. POLICY OBJECTIVES

1.1 The objectives of this policy are to:

- ensure compliance with relevant legislation governing the handling of personal data and the protection of privacy including, but not limited to, the Data Protection Act 1998 and its principles (an overview of key definitions and the principles can be found at Annex 1 of this policy);
- ensure compliance with current HMG Security Requirements for Data Handling;
- ensure that uniform approaches to processing personal data are adopted and applied across all DSA business areas to achieve consistency;
- ensure processes are consistent with accepted codes of practice and guidance including, but not limited to, DSA Information Charter and Privacy Statement; please refer to DSA external website to view these.

2. WHAT IS MEANT BY PROCESSING PERSONAL DATA?

2.1 Any piece of information or data will have an 'information lifecycle' from creation through to destruction. Processing is any operation related to that lifecycle, it will include but is not limited to, the creation, organisation, storage, retrieval, use of, sharing of, disclosure and deletion of personal data.

3. KEY PRINCIPLES FOR PROCESSING PERSONAL DATA

3.1 In order to protect the privacy of an individual and comply with the Data Protection Act, you must ensure that:

- If you collect personal data about an individual (data subject) you let the data subject know why you need it.
- You only ask for what you need and do not collect excessive or irrelevant information.
- The information you hold about individuals is accurate and up to date and that the individuals have the opportunity to correct any details you hold about them.
- You make sure nobody has access to it who shouldn't.
- You let the data subject know if you are going to share their information with anyone else and whether they can say no.
- You only keep personal information for as long as you need it.
- You do not make that information available for commercial use (such as marketing) without permission from the data subject.

- You shall not transfer personal data outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection. (Although the Data Protection Act does not preclude the processing of personal data outside of EEA, where such processing takes place DSA will take steps to assure itself that the processing is secure.)

4. GENERAL RESPONSIBILITIES – ALL STAFF

4.1 Department for Transport, including its agencies, is registered as a single Data Controller with the Information Commissioner (ICO). The statutory Notification, Z7122992, which tells the ICO about the personal data DfT is processing, is maintained by the Data Protection Officer (DPO) for DfT(c). Each Agency has its own DPO (at DSA this is the Data Protection Compliance Manager) and is accountable through its Chief Executive, and ultimately the Secretary of State, for data protection compliance.

4.2 DfT's purposes for holding personal data and a general description of the categories of people and organisations to which DfT may disclose it are listed on the Data Protection Register which can be viewed on the Information Commissioners website. In addition, more details on the organisations DSA shares data with are available on the DfT website through the DfT Information Charter.

4.3 This policy is owned by the Head of Information Assurance. The Knowledge and Information Management Team based in DSA's Information Assurance Branch will carry out periodic reviews of this policy, recommending amendments and variations as appropriate.

4.4 It is the responsibility of all staff, including temporary staff and contractors, Delivery partners and Third Party Suppliers processing personal information on behalf of DSA, to comply with this policy and its requirements.

4.5 IAOs and Contract Managers within DSA who deal with external organisations will take responsibility for ensuring that those organisations sign a contract agreeing to abide by this policy.

4.6 To support staff engaged in the processing of personal data, DSA will also make available further specific information in the form of Standard Operating Procedures (SOP) and background information to staff on the DSA Intranet. This information will include, but will not be limited to, associated DSA policies and procedures in addition to guidance on the relevant legislation and guidance on Government standards for information security.

4.7 DSA has appointed a Data Protection Compliance Manager (DPO) who is responsible for ensuring that data protection is embedded in the key controls and approval processes of all major business processes and functions with the help of the Information Assurance Forum.

4.8 Data protection requirements will also form part of the development of any information security programme for DSA staff.

4.9 Anyone who fails to act according to these responsibilities may be subject to disciplinary procedures as described in the staff handbook.

4.10 Staff must report suspected or actual breaches of this policy by following the Incident Management Procedures or Whistleblowing Procedures (as appropriate).

5. SIRO RESPONSIBILITIES

5.1 The Senior Information Risk Owner (SIRO) will be responsible on behalf of DSA for ensuring that an effective data protection system is established, implemented and maintained in accordance with this policy but has delegated responsibility for the oversight and implementation of this policy to Information Asset Owners (IAO).

6. IAO RESPONSIBILITIES

6.1 IAOs are responsible for identifying and keeping a record of the members of staff and contractors with access to, or involved in, handling individual records containing 'protected personal data'. A definition of 'protected personal data' can be found at Annex 2 of this policy.

6.2 IAOs and Contract Managers within DSA who deal with external organisations will take responsibility for ensuring any existing contractors sign a contract agreeing to abide by this policy and that this policy shall form part of any specification or tender exercise for new contracts.

6.3 IAOs must assume overall responsibility for ensuring that processing of personal data for which they are responsible are managed correctly, appropriately and in compliance with relevant legislation, codes of practice and guidance.

7. INFORMATION CHARTER AND PRIVACY STATEMENT

7.1 DSA knows how important it is to protect privacy and comply with the Data Protection Act and have produced an Information Charter which can be viewed on DSA external website – www.dsa.gov.uk

7.2 The information contained within this policy reflects that which is contained in the Information Charter but provides more specific detail and guidance for staff and contractors.

7.3 DSA Information Charter should be viewed in conjunction with DSA Privacy Statement which is also available on DSA external website.

7.4 It is the responsibility of all staff, including temporary staff an contractors, Delivery Partners and Third Party Suppliers to familiarise themselves with DSA Information Charter and Privacy Statement as this policy should be read in conjunction with both.

8. FAIRNESS

8.1 DSA will inform the data subject why we are collecting their data and what we intend to use it for.

8.2 Where DSA collects sensitive personal data from our customers we will take appropriate steps to ensure that we have explicit consent to hold, use and retain that information. (see Annex 1 for a definition of sensitive personal data)

8.3 DSA will collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or comply with any legal requirements.

8.4 DSA may occasionally be required to process data that is personal, confidential or otherwise considered as sensitive for the purposes of public safety or prevention and detection of crime and, or, the apprehension or prosecution of offenders. Information will be processed for this purpose only where legislation allows, and in accordance with the Data Protection Act 1998.

9. RETENTION AND DESTRUCTION

9.1 DSA will ensure that the information we use is reviewed regularly and is not held for longer that is necessary to fulfil our legal requirements and business needs.

9.2 DSA will have a policy on destruction of personal data and systems/IT equipment processing personal data which sets out how personal data shall be destroyed and which will, in turn, ensure compliance with HMG requirements.

10. RIGHTS OF INDIVIDUALS

10.1 Information must be processed with regard to other legislation such as article 8 of the Human Rights Act which provides that ‘everyone has the

right to respect for his private and family life, his home and his correspondence' If a potential breach of the Human Rights Act is identified the Knowledge and Information Management Team must be consulted for advice.

10.2 DSA will ensure the rights of individuals (Data Subjects) about whom we process information; this includes the right to be informed that processing is being undertaken, the purpose for which that processing is taking place, to whom that information will be disclosed, and, if requested, to receive a copy of that information (Subject Access Request) To comply with the Data Protection Act, DSA must respond to the data subject within 40 days of receipt of the subject access request.

10.3 DSA will ensure the rights of individuals to prevent processing in certain circumstances and to correct, rectify, block or erase information that is regarded as wrong information.

10.4 Where third party information may be disclosed in the course of responding to a subject access request, DSA will usually consult with that individual prior to any decision being made on disclosure.

10.5 DSA staff will be given guidance and procedures on handling subject access requests and DSA will provide potential applicants with information about subject access requests on its external website and on request by telephone, email or by other written communication; this will include how to make a valid request or complaint and any relevant charges or verification details required in relation to that request.

10.6 DSA will reserve the right to make the maximum £10 charge for subject access requests as provided for under the Data Protection Act.

10.7 Where disclosure of staff information, for example, name and job title, may be released as part of a subject access request, DSA will not release that information without first considering the public interest in that disclosure, as a general rule, however, details of individuals of a grade sufficient enough to be in the public domain (i.e. Grade7and above) will be released.

10.8 DSA will ensure that, where possible, subject access requests are responded to in the format requested by the data subject.

10.9 DSA will have a complaints procedure in place for our customers and data subjects. Details of DSA complaints procedure and service standards are available on request from DSA and on DSA external website. Further information can also be found in the DSA Information Charter which can also be viewed on the external website; DSA Knowledge & Information Management Team will be responsible for reviewing and updating the Information Charter.

11. SECURITY

11.1 DSA will have in place an 'Appropriate use of IT and Communications Equipment Policy' to cover the appropriate use of DSA equipment and all forms of electronic communication. This policy can be viewed on DSA's Intranet.

11.2 DSA will strive to comply with the ISO 27001 standard and government standards for information security, as a minimum.

11.3 DSA is required to report to DfT on matters relating to HMG IA Standard No.6, the Security Policy Framework (SPF) and Information Assurance Maturity Model (IAMM)

11.4 The SPF sets out minimum security policies that Government Departments and Agencies must adhere to; DSA will handle classified information in accordance with the SPF.

11.5 The IAMM is a model to assist a Government Departments and Agencies in putting in place an effective change programme to improve risk management; this will include, but is not limited to, policies to back up systems and prevent accidental loss.

11.6 DSA will manage its information to ensure appropriate levels of security and accessibility (letting the right people have access to the right information).

12. DISCLOSURE

12.1 DSA may occasionally be required, by law, to disclose certain types of information that is personal, confidential or otherwise considered as sensitive; it is DSA policy, however it is processed, whether on paper, electronically or by other means to protect the rights and privacy of individuals in accordance with the Data Protection Act 1998.

12.2 DSA will not disclose personal data to anyone outside DSA or other body where it may be shared internally with those who need it in order to carry out their business, or where it would be compatible with the purpose for which it was collected; except where legislation allows. This will include but is not restricted to subject access requests and section 29 and 35 disclosures (see below) See also section on Data Sharing and, for information about access to your own data or disclosure of third party data, see section on rights of individuals.

12.3 A section 29 disclosure is where a disclosure is made by DSA to another party, for example police, for any of the following purposes:

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of any tax or duty or any imposition of a similar nature.

12.4 A section 35 disclosure is where a disclosure is made by DSA to another party, for example solicitor, where disclosure is necessary:

(a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or

(b) for the purpose of obtaining legal advice,

or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

12.5 It is DSA policy not to disclose personal information under s29 or s35 unless DSA are satisfied that the request meets s29 or s35 criteria and that there are no exceptional circumstances that would prevent disclosure. The Knowledge & Information Management Team can provide advice where necessary.

13. DATA SHARING

13.1 A data sharing activity takes place when DSA provides any data it holds, for example, commercial (non-personal), personal data or a combination of both to another party (usually an external party or organisation) for the purposes of fulfilling a statutory requirement or for the purpose of achieving the business objectives of a particular project or other business interest. A data sharing activity can involve bulk sharing where more than one record is shared or the sharing of an individual record; it can be in relation to a one off request or involve regular sharing. For further detail, please refer to DSA's Data Sharing Policy.

14. COMPLIANCE

14.1 This policy and any other related policies, guidance or standard operating procedures applies to all staff including temporary or contract staff and any Delivery Partner or Third Party Supplier processing personal data on behalf of DSA.

ANNEX 1

Glossary of Terms and Definitions

"personal data" means data which relate to a living individual who can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

"sensitive personal data" means personal data consisting of information as to—

(a) the racial or ethnic origin of the data subject,

(b) the political opinions of the data subject

(c) the religious beliefs or other beliefs of a similar nature of the data subject,

(d) whether the data subject is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),

(e) the physical or mental health or condition of the data subject,

(f) the sexual life of the data subject,

(g) the commission or alleged commission by the data subject of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

"data controller" means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

"data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

'third party' means an individual/organisation other than the data subject, the data controller or its agents. This is a term defined in the data protection act 1998 and should not to be confused with a 'third party supplier' (a third party supplier is a commercial entity contracted to supply services to government).

"processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available,

Or

(d) alignment, combination, blocking, erasure or destruction of the information or data;

'data subject' any living individual who is the subject of personal data held by an organisation.

'**Subject Access Request'** a request made by an individual to the DSA for information about, or a copy of, their personal data.

'DSA customers' any person that is not an employee of DSA who uses DSA as a regulatory authority, as a service or for information.

'**Senior Information Risk Owner (SIRO)'** the SIRO is an executive and member of the Executive Board familiar with information risks and is responsible for leading and fostering a culture that values, protects and uses information for the public good. The SIRO owns the overall information risk policy and risk assessment process and ensures that it is used.

'Information Asset Owner (IAO)' Information Asset Owners are senior individuals involved in running the relevant business area. Their role is to understand what information asset is held, what is added, what is removed, who has access and why; in general terms the 'lifecycle' of their information assets from creation to destruction. The IAO will provide written input to the SIRO annually on the security and use of their information asset.

The Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

ANNEX 2

MINIMUM SCOPE OF PROTECTED PERSONAL DATA

Departments must identify data they or their delivery partners hold whose release or loss could cause harm or distress to individuals. This must include, as a minimum all data falling into one or both of the categories below.

Any information that links one or more identifiable living person with information about them whose release would put them at significant risk of harm or distress.

1. one or more of the pieces of information which can be used along with public domain information to identify an individual	**Combined with**	**2. information about that individual whose release is likely to cause harm or distress**
Name/address (home or business or both)/postcode/email/telephone numbers/ driving licence number/date of birth. [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]		Sensitive personal data as defined by s2 of the Data Protection Act including records relating to the criminal justice system, and group membership. DNA or finger prints/ bank, financial or credit card details/ mothers maiden name/ National Insurance number/ Tax, benefit or pension records/ health records/ employment record/ school attendance or records/ material relating to social services including child protection and housing

These are not exhaustive lists. Departments should determine whether other information they hold should be included in either category.