Driver and Vehicle Licensing Agency (DVLA)

Data protection audit report

Executive summary
May 2016

Information Commissioner's Office

1. Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

1.3 The Driver and Vehicle Licensing Agency (DVLA) has agreed to a consensual audit by the ICO of its processing of personal data.

1.4 An introductory meeting was held on 18th September 2015 with representatives of the ICO and the DVLA to identify and discuss the scope of the audit.

2. Scope of the audit

2.1 Following pre-audit discussions with the DVLA, it was agreed that the audit would focus on the following areas:

a. **Security of personal data** – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

b. **Data sharing** - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

The engagement between the ICO and the DVLA has been split into two audits. Audit One was focused on the following services:

- Insurance Industry Access to Drive Data (IIADD) or 'MyLicence'
- View Driving Licence (VDL) / Check Driving Licence (CDL)
- Electronic Driver Entitlement Checking Service (EDECS) and Access to Driver Data (ADD)

Audit Two was focused on the following service:

- Disclosure of vehicle keeper data for private parking enforcement

3. Audit opinion

3.1 The purpose of the audit is to provide the Information Commissioner and the DVLA with an independent assurance of the extent to which the DVLA, within the scope of this agreed audit, is complying with the DPA.

3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
High Assurance	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with the DPA. We have made four high assurance assessments of the control areas reviewed across the two audits.

4. Summary of audit findings

4.1 Areas of good practice

- There is a Data Governance Board in place which is the key corporate committee for the management of information security. Its membership includes all the key stakeholders from across the Agency. The Board receives a monthly dashboard of statistics around, amongst other things, data breach volumes, system accreditations and audit, and IT intrusion detection system reports. The Board also manages its own risk register which forms part of the Agency's overall risk management approach.

- There is mandated annual refresher training in place for all staff on information security. The Information Assurance Group (IAG) produces this training in-house and varies the format from year-to-year to keep staff engaged and it monitors completion by staff. The Agency had a completion success rate of 99.6% during the last calendar year.

- There is a clear access control process in place for all users of Agency IT systems. Access is granted to users on a "need to know" basis. Reviews of basic access rights are carried out at least once every six months as part of the Continued Business Need process. For users with privileged access rights, access is reviewed at least once every three months by the Service Desk, as part of the Privileged Access Revalidation process.

- Physical security risk assessments are undertaken on an annual basis and the Agency has in place a number of robust perimeter and entry controls. These are further enhanced for any staff member or visitor requiring access to the Data Centre.

- There is a comprehensive Data Breach Policy and Procedure in place. All data breaches and near misses are recorded on a log and the manager in the local business area is required to provide a comprehensive written account of the breach, alongside remedial actions to avoid a reoccurrence. The number of incidents are included in the Annual Information Security

Statement written by the SIRO and provided to the Chief Executive.

- There is a clear data sharing clearance process in place which the Data Sharing Assurance Team maintain responsibility for to ensure no personal data is provided to external parties without IAO clearance. A Data Sharing Clearance Panel convenes on a regular basis to consider each request, their review includes an assessment of the legality of the information sharing proposed, how it will be shared and any security considerations. Any risks or concerns raised are documented alongside the Panel's view to approve or reject the information sharing request.

- There are high-level contractual agreements in place for all data customers using EDECS and ADD. The Data Sharing Agreement sets out common rules for the recipient of the data to follow. The common rules set out in the agreement include permitted purpose for use, data security and retention of records.

- There is a Keeper of Data at Event (KADOE) contract in place for all private parking companies, intermediaries and link providers. The data sharing agreement contains a dedicated section on data security, alongside a schedule that details very clearly the specific security requirements a company must have in place to have access to keeper data. Provisions for the DVLA to audit the company are also set out within the contract.

- Private parking companies, intermediaries and link providers must complete an annual data governance and contract compliance assessment. This is a self-assessment questionnaire which requests the company to confirm data governance and compliance with the terms of the contract. Companies are required to notify the DVLA of the outcome within 28 days of conducting the checks.

- There is a secure file transfer protocol in place for the sharing of DVLA vehicle keeper data via a business-to-business (B2B) gateway. The gateway validates customer enquiries through unique codes, data can only be sent between two fixed IP addresses and private parking companies log into the gateway through a unique service user ID.

- The Personal Information Charter displayed on the DVLA's website provides information to individuals about the circumstances in which their data may be released. There is further information in the DVLA's Release of Information booklet. The booklet details the reasons for releasing data to private car parking companies and provides a FAQ section towards the end of the document. The FAQ's include the ability to release information to private companies and how this data is requested.

4.2 Areas for improvement

- Audit and assurance activity on third parties accessing DVLA data through the ADD service is mainly undertaken remotely; therefore there maybe scope to increase the amount of tier 3 audit activity undertaken by Government Internal Audit Agency (GIAA) auditors through site inspections.

- Whilst there is a dedicated training programme for all staff on information security, specific data sharing based training is not delivered generally to all staff. The DVLA should ensure that specific data sharing training is provided to all staff involved in making informed decisions regarding data sharing or disclosures of data.

- Adequate fair processing information is not provided to individuals who need or choose to use the VDL service via the telephone. A script should be in place to ensure individuals receive this information.

- GIAA also complete tier 3 audit work on behalf of the DVLA on private parking companies. They are primarily focused on ensuring requests for keeper data can demonstrate evidence of meeting reasonable cause criteria. Whilst there is also a degree of focus on data security arrangements we believe this element of the audit activity could be further enhanced to ensure companies remain compliant with contractual obligations in regards to data security.

- Staff who process manual requests for keeper data during a company's probation period are largely trained through on-the-

job training and guidance from more experienced staff members within the team. We believe there is scope to implement specific training for staff involved in deciding whether the reason for requesting data falls under reasonable cause. The training should include detailed information on when it is appropriate to release data and an overview of the operating instructions currently in place.
