

PRIVACY IMPACT ASSESSMENT

PROJECT NAME:	Continuous Insurance Enforcement (CIE)
PROCESS DESCRIPTION:	Draft by Project review by Internal and External Stakeholders

PIA manager:	David Hancock	Position:	Communications, Stakeholder and Policy Workstream
--------------	---------------	-----------	---

Date PIA started:	1 st PIA April 2009.
-------------------	---------------------------------

Stage 1 ► Preparation for screening

1.1 Purpose and objectives of the project or process

All vehicles used on the road or public place must be covered by valid third party motor insurance. It is currently an offence to use a vehicle with no insurance and in the future it will also be an offence to keep a vehicle with no insurance. Registered keepers will therefore need to ensure that their vehicles are continuously insured (unless specific exemptions apply) or expect enforcement action to be taken.

Section 144A of the Road Traffic Act 1988 (which results from section 22 of the Road Safety Act) states "If a motor vehicle registered under the Vehicle Excise and Registration Act 1994 does not meet the insurance requirements, the person in whose name the vehicle is registered is guilty of an offence."

The scheme for continuous insurance and its enforcement ("Continuous Insurance Enforcement" or "CIE") intends to identify uninsured drivers from the keeper record held by Driver and Vehicle Licensing Agency (on its Vehicle Software System or "VSS") and the insurance industry's database of motor vehicle policies (the Motor Insurance Database or "MID").

The implementation of CIE is one of DVLA's Secretary of State targets. Its target is to 'Introduce Continuous Insurance Enforcement and to have started to issue Insurance Advisory letters by 31 March 2011'.

The scheme consists of 2 main processes:

1. Compliance - providing opportunity for keepers to become compliant
2. Enforcement – taking enforcement action against those that are non compliant

Compliance starts with education and awareness, informing individuals, specifically registered keepers, of their obligation to continuously insure their registered vehicles. Before the scheme becomes operational there will be a period of education and awareness to ensure that the public are aware that the registered keeper is responsible for ensuring the vehicle is continuously insured.

The campaign will utilise a variety of media forms to re-enforce the message to reach as wide an audience as possible, recognising that differing audiences will respond to different media forms.

It is expected that a publicity campaign and increasing awareness will improve compliance ahead of any release of insurance advisory letters and the introduction of enforcement.

Eligible registered keepers of vehicles identified from the database comparison without insurance will initially receive an insurance advisory letter outlining a number of options and actions they need to take to become compliant. These include: ensure their insurance provider has updated the MID, purchase insurance or notify a change of keeper or some other appropriate update to DVLA such as declaring Statutory Off Road Notification (SORN). This insurance advisory letter will be issued by the Motor Insurer's Bureau (MIB), and continued non-compliance will ultimately lead to enforcement action being taken by DVLA.

DVLA will carry out enforcement activities through fixed penalties, court prosecution and/or being identified for wheel clamping. Enforcement will use existing DVLA processes, updated/amended to take into account specific requirements of CIE.

The database comparison process will enable identification of those who continuously or repeatedly offend (via the Vehicle Registration Mark (VRM) and Keeper details); DVLA may decide a different enforcement approach for example court prosecution rather than another fixed penalty notice.

On road police enforcement against uninsured drivers will continue. It is likely that successful DVLA enforcement activity should allow the police to focus more on hardened insurance evaders i.e. those that continue to drive the vehicle in spite of all warnings.

1.2 Preliminary assessment of data usage

1.2.1 What kind of personal information is to be used?

MIB will supply DVLA with an extract of the MID database – a list of VRMs with insurance cover on a stated date – monthly.

MIB will provide to DVLA the following data:

VRM
Make-model (where available on the MID)
Post Code
Policy Number
Insurer ID

DVLA will compare this extract with an extract from VSS covering the same dates as the MID extract. For those VSS records that do not match MID records initially, DVLA will carry out a second comparison exercise to

identify possible mistypes, cherished transfers (for example personalised number plates) and any fleet anomalies (for example where an open policy covering all fleet vehicles for a company has been issued but the VRM has simply not be entered onto the MID) on MID records to ensure the process correctly identifies those we believe to be uninsured. It is proposed MIB carry on this secondary comparison at a future point.

DVLA will initially provide to MIB the following data:

DVLA – VRM

MIB – VRM

Date

Reason – Code

Make – Code

Make - Description

DVLA – Fleet no (where appropriate)

DVLA - Date last keeper change

DVLA – Tax Class

DVLA - Body Type

DVLA – Wheel plan

DVLA – Date Of Liability

DVLA – Outbound part of the postcode

Policy Number

Insurer ID

DVLA will also supply the MIB – VRM, Insurance Policy Number and Insurers' Code from the original list provided by MIB if DVLA are able to identify possible mistypes or cherished transfer anomalies (via the second comparison) with the expectation that insurers will take corrective action.

Keepers name and address details will be requested by MIB if an Insurance Advisory letter is about to be sent (24 Hrs before) having checked the current insurance status of a vehicle on the MID first. The information shared between DVLA & the MIB will be kept to the minimum required to ensure the process is robust, efficient, minimally intrusive and meets legislative requirements.

1.2.2 How will it be collected?

The MID extract will be sent by the KCOM, MIB IT supplier to DVLA through the ELISE (Electronic Links, Implementation and Strategic Enablement) gateway, resilient, business to business (B2B) connection – monthly.

The ELISE gateway aims to replace numerous disparate connections between third party organisations and the DVLA via the delivery of a common communications platform. The capability of the services provided by the gateway is demonstrated and proven from other projects undertaken with DVLA strategic partners. Tactically the Agency wants to use ELISE in its vulnerable electronic links with its partners and customers. Strategically ELISE will also provide the ability to quickly and efficiently offer standard external data exchange services, such that the

DVLA can take a pro-active and cost effective approach to meeting future trading partner's requirements.

The B2B services implemented via the gateway are supported across a well-defined technology set. Analysis of current and future trends, together with advice from the DVLA Technical Design Authority, indicate that the implementation of business services within the following technologies will satisfy the known DVLA customer base:

- Ø IBM Message Queue (MQ)
- Ø Web services
- Ø Secure file transfer.

CIE business processes will utilise all three of these technologies.

Following a comparison of the VSS extract and the MID extract, within DVLA, the Insurance Advisory pool will be sent to MIB through ELISE as above – monthly.

Keeper information held on VSS will be sent to MIB via ELISE. This information will be requested by the MIB daily using a batch file process, the day before an insurance advisory letter is to be sent out.

The transfer of data to and from DVLA will be via the IBM Message Queue (MQ).

Throughout the process the DVLA's Code of Connection (CoCo) standards and requirements for security will contractually be applied by all parties.

1.2.3 Who will have access to it?

DVLA and the MIB (or their agents) will be the only parties with access to the data. DVLA will supply MIB with a list of eligible vehicles on a monthly basis. This information will be stored within the MIB's bespoke built system, the Comparison System, and updated monthly.

The Compliance System will hold keeper details until:

1. The "Keeper" becomes compliant or,
2. DVLA instruct MIB to close the case

The MIB Compliance System will use the data to issue Insurance Advisory Letters and handle any queries directed to the MIB.

The MIB and DVLA will only keep appropriate levels of data for the minimum period required for the processes of compliance and enforcement to be effective. MIB wish to retain some data for trend analysis with a view to enhancing the effectiveness of the scheme in the public's interest.

This information will not be used for any purpose other than

understanding the drivers who evade insurance.

1.2.4 How will it be transmitted to any third parties?

Daily/Weekly batch via ELISE – secure B2B gateway.

1.2.5 How will it be stored, kept up to date and disposed of when no longer required?

An individual’s case will close automatically once the record is updated to show the vehicle has become compliant or is not in scope of the scheme and therefore not eligible for possible enforcement action.

It has been agreed that the MIB can keep Name/Address for a period up to 24 months. This is to help the MIB identify persistent offenders and help in the handling of queries when the keeper receives an Insurance Advisory letter and is based upon the need to identify those seeking to manipulate the annual nature of tax and insurance cycles.

Retention and deletion schedules will be agreed between all parties and within business need requirements of DPA.

1.3 Preliminary stakeholder analysis

Stakeholder name	Their interest in the proposal
External: Vehicle Keepers	
Courts/CJS	Will receive additional workload
Wheelclampers	Will receive additional workload
Police	Free up police time to focus on hardened evaders. Provide more accurate data
ABI	Representative body of Insurers.
Fleet Operators	Ensuring burdens are minimised in supporting the new regime. Awareness for members.
AA/RAC	Representing vehicle keepers
Vehicle Leasing Organisations	Ensuring burdens are minimised in supporting the new regime. Awareness for members.
Internal: Customer Enquiry Group	Will receive additional workload
VCS	Will receive additional workload
DfT	Providing funding for the solution
Enforcement Directorate	Will receive additional workload
NB: MIB are a party to this process and therefore not considered to be a stakeholder in this sense.	

1.4 Environmental Scan

CIE builds on recent experience of implementing Continuous Registration (CR), which has tightened the enforcement of Vehicle Excise Duty (VED),

from the DVLA vehicle record. There are essential differences.

- the main beneficiaries from CIE will be the responsible motorists as the number of uninsured drivers on the road will be reduced, thereby lessening the chance that they could be involved in a collision with an uninsured vehicle, road safety improvements and reduced requirements for insured motorists to subsidise those that drive without insurance.
- the statutory basis differs from that for VED enforcement
- the average insurance premium is some three times more expensive than average VED rates so offenders may be less willing to comply. [REDACTED]. This highlights the fundamental need for both preventative measures from the record and effective 'on road' enforcement.

Stage 1 completed by:		Date:	21/1/10
-----------------------	--	-------	---------

Stage 2 ► Screening

The questions below, which are based on those used in the ICO's PIA Handbook, have been used to help determine whether a PIA is necessary and, if so, how extensive it needs to be.

2.1 Technology

2.1.1 Will there be new or additional information technologies that have substantial potential for privacy intrusion?

No additional technologies are being used by DVLA.

The DVLA CoCo will stipulate security (and other) requirements for MIB before they can connect to ELISE b2b gateway to be used for data transfers between MIB and DVLA.

2.2 Identification methods

2.2.1 Will there be the creation of new identifiers or re-use of existing identifiers?

DVLA will provide the MIB with VRMs for which there is no corresponding insurance policy on MID.

DVLA will provide MIB with VRMs (CT, Mismatches, Fleet)

At the appropriate point, MIB will request names and addresses of registered keepers that are non-compliant and those keepers will be sent an Insurance Advisory letter by the MIB.

2.2.2 Might there be identification of individuals who were previously anonymous?

Yes, Non-compliant keepers will be identified by DVLA and sent Insurance

Advisory letters by the MIB, expected to be around 80,000 a month once fully operational.

Compliant keepers will not be identified and will not receive Insurance Advisory letters.

The MIB and DVLA are working to improve the integrity of data used before “go live” to minimise the possibility of any compliant keepers receiving Insurance Advisory letters in error

2.2.3 Will there be new or substantially changed identity authentication requirements that may be intrusive or onerous?

There is no change to identification requirements, which are based on current use of keepers and insurance data.

2.3 Involvement of multiple organisations

2.3.1 Will the initiative involve multiple organisations, whether they are government agencies (e.g ‘joined-up government’ initiatives) or private sector organisations (e.g as outsourced service providers or as business partners?)

Yes

Government:

DVLA

Courts

Police

Private:

IBM/Fujitsu (DVLA IT Provider)

MIB (and IT partner)

Experian (for MID)

Wheelclamping Contractor.

2.4 Changes to the way data is handled

2.4.1 Will there be new or significant changes to the handling of types of personal data that might be of particular concern to individuals? This could include information about racial and ethnic origin, political opinions, health, sexual life, offences and court proceedings, finances, and information that could enable identity theft.

Yes, Non-compliant keepers of vehicles will be identified to MIB and sent Insurance Advisory letters.

Data Security is paramount to protect the privacy of individuals to prevent it falling into the wrong hands – during transmission between DVLA and MIB, and where it resides at MIB before it is deleted. The processes developed will cater for strict governance over B2B requirements and access rights.

2.4.2 Will the personal details about each individual in an existing

database be subject to significant new or changed handling?

Yes, it involves large-scale matching of data to identify individuals that are potentially breaking the law. Access rights to be agreed.

2.4.3 Will there be new or significant changes to the handling of personal data about a large number of individuals?

Yes, MIB or its nominated IT supplier, will transfer approx 34 million insurance records (minimal information not the whole record) to DVLA for the initial matching to be carried out, and DVLA will be transferring to MIB name and addresses for non-compliant registered keepers if they are to be sent a Insurance Advisory letter. This is currently expected to be 1.4m records in first 12 months. (Not necessarily unique keepers, some could become non-compliant several times during a year).

2.4.4 Will there be new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

If there is a full match between a VRM held by DVLA and a VRM on the MID, it means that the registered keeper has an insurance policy for that vehicle and therefore no further action is warranted. However, if the DVLA VRM does not match the VRM on the MID, a second comparison will be carried out to establish possible matches to a MID VRM.

The second comparison will reveal if a DVLA VRM has a:-

- Fleet identifier number shown on VSS record (that is we know that there is an open cover policy for the company which covers all its vehicles) These VRMs are sent to the MIB as possible anomalies (for example the company's vehicle is insured but the VRM has not been entered onto the MID).
- Cherished Transfer Marker shown on VSS record within the last 12 months and the most recent VRM matches a VRM in the List of Insured vehicles AND the Make and Postcode are the same as the record in the List of Insured Vehicles (MID). The VSS VRM and possible MIB VRM match are sent to the MIB as possible Cherished Transfer anomalies.
- Where DVLA has identified a possible mistype where the Make and Postcode match a MID record in the List of Insured Vehicles and The VSS VRM matches on more than 4 characters of the VRM of the record in the List of Insured Vehicles

Where there is no match identified following the second comparison exercise, DVLA will determine the vehicle as being non-compliant and send the VRM to the MIB. After a configurable period of time, if the record shows the VRM continues to be non-compliant, the MIB will send the "Registered Keeper" an Insurance Advisory letter.

Fleet anomalies, cherished transfer anomalies and mistypes will initially receive a different letters.

2.5 Changes to data handling procedures

2.5.1 Will there be new or changed data collection policies or practices that may be unclear or intrusive?

There are no changes to the ways in which the data is collected.

2.5.2 Will there be changes to data quality assurance processes and standards that may be unclear or unsatisfactory?

The DVLA/MIB is improving the integrity of both databases and the data exchange process includes several iterations to allow for latency issues between both databases.

2.5.3 Will there be new or changed data security arrangements that may be unclear or unsatisfactory?

No, the CoCo will be agreed by both sides, produced by DVLA and signed up to by MIB.

2.5.4 Will there be new or changed data access or disclosure arrangements which may be unclear or permissive?

No, the CoCo will provide DVLA with assurance that MIB as a non-governmental connecting organisation meets industry best practice with regards to Information Security.

2.5.5 Will there be new or changed data retention arrangements that may be unclear or extensive?

It has been agreed that the MIB can keep Name/Address for a period up to 24 months. This is to help the MIB identify persistent offenders and help in the handling of queries when the keeper receives an Insurance Advisory letter. Details of this will be in the Operational SLA and data usage will be subject to open scrutiny by DVLA audit and comply with the following legislation:-

The Data Protection Act 1998

The Human Rights Act 1998

The Regulation of Investigatory Powers Act 2000

The Lawful Business Practice Regulations 2000.

2.5.6 Will there be changes to the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?

CIE will not use any new means of disclosing data that are not already employed by DVLA in support of its business and providing services. All media used for CIE is already employed by DVLA for other purposes.

2.6 Statutory exemptions/protection

2.6.1 Will the data processing be exempt in any way from the DPA or other legislative privacy protections? This might apply in areas such as law enforcement or public security

The CIE process is not exempt to the DPA or any other legislative privacy

protections.

2.6.2 Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

No, all parties, including commercial partners, will fully meet the requirements of the Data Handling Review and Cabinet Office guidelines on data sharing.

2.7 Justification

2.7.1 Does the project's justification include significant contributions to public security measures?

No, just road safety.

2.7.2 Is there to be a full 12-week public consultation?

A 12 week public consultation was conducted by Department for Transport where Privacy matters were considered, it closed in April 2009.

2.7.3 Is the justification for the new data handling unclear or unpublished?

No. The public consultation document included reference to the need for handling of data.

Stage 2 completed by:

Date:

21/1/10

Stage 3 ► Outcome of screening

3.1 Preliminary identification of risks

The table below lists the key privacy risks that have been identified by the screening process.

	Description of risk	Preliminary assessment of exposure
Risk 1	An Insurance Advisory letter is sent to an individual who is actually compliant, causing irritation, and possible stress and anxiety. This could also cause reputational harm to DVLA if it occurred on a large-scale.	L
Risk 2	Public perception that the processing is excessive and unfair in terms of the DPA if the number of non-compliant keepers is relatively low.	L
Risk 3	Potential to lose personal data in transfer from DVLA to MIB or that the data could be corrupted en route.	L
Risk 4	Personal data is provided to MIB / their processor and subsequently misused for another purpose without DVLA authority / knowledge	L

Risk 5	Risk that the personal data may be lost or corrupted by MIB provider (Experian)	L
---------------	---	---

3.2 Decision on how to proceed

Given the volume of data being transferred and matched, and the number of individuals that could be affected by this project, together with the fact that the project is subject to a public consultation, a full-scale PIA would be beneficial.

Having completed the screening process and identified privacy risks, we have concluded that continuation of this PIA is warranted. This has been discussed with and agreed with the data protection officer.

Name of decision officer	
Name of DPO who agreed with this decision	

Stage 3 completed by:		Date:	21/1/10
-----------------------	--	-------	---------

Stage 4 ► Preparation for the consultation and analysis

4.1 Governance arrangements

The PIA will continue to be managed as part of the Continuous Insurance Enforcement Project. The following individuals will, through the project team, be involved in the process.

Name	Their role
	PIA and Project Manager
	Data Protection/Privacy Officer
	Technical IT Security Manager
	Information Assurance Group

4.2 Stakeholders to be consulted

Stakeholder: Name / role / organisation	What interests do they have in the proposal?	How are you going to consult with them?
Customer Enquiry Group/DVLA	To ensure there is not a significant impact on the contact centre due to CIE and that they are able to answer questions raised by the public in relation to the use of their data and their privacy concerns.	Attends the relevant workshops and CIE monthly checkpoint meetings. Also receives monthly checkpoint report.
David Hancock/CIE Project Executive/DVLA	David Hancock has overall responsibility for the project and is Director of Enforcement	David Hancock has regular meetings with the Project manager and team and chairs CIE2 Project

	Directorate.	Board.
DVLA Policy/DVLA	To ensure that the release of information conforms with the DPA	Policy attend relevant workshops and are consulted with.
Road Worthiness Insurance Division, DfT	lead for DfT policy. DfT are funding the Project.	sit on CIE2 Project Board and are regularly consulted when advice or decisions are needed.
IT Security/DVLA	has responsibility for ensuring CIE complies with IT Security Standards.	All relevant documents are sent to IT Security for Quality Assurance. IT Security attend the relevant workshops and CIE monthly Checkpoint meetings. Also receives the monthly checkpoint report
Technical Authority/DVLA	has responsibility for ensuring that DVLA systems and data are delivered and operated in a safe and secure manner.	All relevant documents are sent to TA for Quality Assurance. TA attend the relevant workshops and CIE monthly Checkpoint meetings. Also receives the monthly checkpoint report
Service Management/DVLA		Service Management attend relevant workshops and are consulted
Head of MID Services/MIB	has overall responsibility for CIE within MIB and is responsible for the management and security of the data once transferred from DVLA to the MIB and for ensuring the correct non-compliant individuals are identified	Regular communication via checkpoint and MIB and DVLA Project Board and DfT Steering Group meetings. We will also meet face to face when necessary.
DVLA	Accreditation	IAG attend relevant workshops and are consulted.

Internal Stakeholders	What interests do they have in the proposal?	How are you going to consult with them?
	Ensuring compliance with the DPA	Policy attends relevant workshops and is regularly consulted with.
	Departmental PIA Lead,	Meetings or through

	and DPO for DfT(c)	correspondence
Head of Information Security (Involve where there are information security issues)	Ensuring compliance with the departmental information security standards, to the extent that they impact on privacy issues	IAG attend relevant workshops and are regularly consulted with.
DfT Legal (Involve where there are complex legal compliance issues)	Ensuring compliance with any relevant legislation	DfT Legal are consulted

4.3 Consultation Plan

A Consultation Exercise, covering privacy issues, was conducted by DfT in January 2009. The proposals for CIE were subject to a 12 week public consultation which closed on 16 April 2009. A total of 67 responses were received to the consultation, 32 of which were received from organisations or representative bodies and 35 from individuals.

There are stakeholder meetings held on a six monthly basis where privacy of information is agenda item.

Full details are available at www.dft.gov.uk/consultations/closed/motor/

4.4 Resources

No additional resource requirements

Stage 4 completed by:		Date:	21/1/10
-----------------------	--	-------	---------

Stage 5 ► The Consultation

5.1 External stakeholders

Stakeholder name	The privacy issues they raised
Information Commissioners Officer (ICO)	<p>The ICO felt the PIA was a good example of PIAs being put into action. The consideration given to the impact CIE is going to have and the risk mitigations, that provided clear direction for the project, was praised.</p> <p>The ICO felt that due to the need to tackle uninsured drivers the risk analysis and mitigations suggest to it is a proportionate response to the problem.</p> <p>The ICO commented</p> <ul style="list-style-type: none"> - that it was useful that the organisations have looked at the comms/PR aspects of the project at an early stage, outlining plans to undertake an awareness campaign. - DfT has taken the right approach in terms of the level of

	<p>data sent to MIB for the suspect pool. In particular, DVLA will not be sending the name and address of a driver due to receive a letter until it is necessary for MIB to have that information. This will help to prevent excessive levels of personal data relating to compliant drivers from being stored on the suspect list.</p> <p>The main concern about the accuracy of the information is the problems caused by delays in insurance details being entered onto the MIB database. This can result in drivers appearing to be uninsured when this is not the case; my understanding is that at any given time, approximately 3% of the information on the database is inaccurate. The PIA addresses this by stating that details will have to remain in the 'suspect pool' for a certain number of cycles. This seems to be a suitable approach, and should minimise the number of false reports.</p>
--	---

5.2 Internal stakeholders

Department for Transport (DfT)	DfT has been part of the review process since the initial version was produced. DfT have provided comments and these have been incorporated into the document. DfT also sits on the CIE Steering Group and Project Board so can reflect their views.
Enforcement Directorate (ED)	Enforcement Directorate has been part of the review process since the initial version was produced. ED have provided comments and these have been incorporated into the document. David Hancock, Director of Enforcement and E Services is also CIE Project Executive so has a wider view.
DVLA Policy	Policy has been part of the review process since the initial version was produced. Policy have provided comments and these have been incorporated into the document.
IT Security	IT Security has been part of the review process since the initial version was produced. IT Security have provided comments and these have been incorporated into the document.
Information Assurance Group (IAG)	IAG has been part of the review process since the initial version was produced. IAG have been provided comments and these have been incorporated into the document.

NB: do not include members of the Project or PIA team

Stage 6 ► Compliance with privacy laws

The following privacy laws are relevant to this project and so have been considered as part of this PIA.

6.1 Data Protection Act (DPA)

A DPA compliance check has been carried out as part of this PIA (attached at annex A) and we are content that the initiative can work successfully whilst complying with the requirements of the DPA.

6.3 Human Rights Act (Article 8)

There are no special considerations under the HRA. The processing is in accordance with regulation 27 of the Road Vehicles (Registration and Licensing) Regulations 2002 for the exercise of s144A of the Road Traffic Act 1988.

6.4 Privacy and Electronic Communications Regulations (PECR)

N/A

6.5 Regulatory and Investigatory Powers Act (RIPA)

N/A. Personal data will not be processed under RIPA.

6.6 Common Law duty of confidence

N/A. There is a statutory power for the disclosure of the information

6.7 Others (such as provisions within statutes which govern the activities and programmes of Govt agencies)

Regulation 27 Road Vehicles (Registration and Licensing) Regulations 2002, s144A Road Traffic Act 1998.

Stage 7 ► Risk analysis

The table below shows the key privacy risks that have been identified, and the options for avoiding or mitigating those risks.

RISK REGISTER FOR PRIVACY IMPACT ASSESSMENT

If the identified risks in 3.1 are agreed, they should be copied here, and mitigation assessments made, as standard risk policy.

Risk description	Inherent Privacy Risk			*Options for avoiding or mitigating this risk	Residual Privacy Risk		
	Impact	Likelihood	Exposure		Impact	Likelihood	Exposure
An Insurance Advisory letter is sent to an individual who is actually compliant, causing irritation, and possible stress and anxiety. This could also cause reputational harm to DVLA if it occurred on a large-scale.	H	L	H	Mitigation: Focus on improving accuracy of data. DVLA only release name and address of keeper if they have satisfied themselves through “anomaly” checks that probability of incorrect targeting is very low.	H/M	L	H/M
Public perception that the processing is excessive and unfair in terms of the DPA if the number of non-compliant keepers is relatively low.	L	L	L	Mitigation: Education and awareness campaign to ensure that the public understands the current high level of evasion and the forecasted increase to the numbers of uninsured vehicles should we adopt a “do nothing” approach	L	L	L
Potential to lose personal data in transfer from DVLA to MIB or that the data could be corrupted en route.	H	L	L	The use of SFTP between DVLA and MIB ensures that the identity of the receiving system is authenticated before the transfer commences. These transfers are being made across the secure C&W Closed User Group (CUG) connection. The risk of data corruption remains; the use of header/footer records and ‘end of transmission’ files has been introduced to ensure that major corruptions are captured, allowing corrective action to be taken. Further investigation is planned to take place to ensure that minor corruptions or data issues in individual records are captured.	H	L	L

Personal data is provided to MIB / their processor and subsequently misused for another purpose without DVLA authority / knowledge	H	L	L	The DVLA-MIB SLA document sets the guidelines for MIB's use of DVLA data (and vice versa) – previous discussions with DVLA's Head of information Security has indicated that it is not feasible for DVLA to continually audit all parties that hold their data, instead they must trust that the applicable contracts / SLAs / Data Protection Act is being followed.	H	L	L
Risk that the personal data may be lost or corrupted by MIB provider (Experian)	H	L	L	For the 'core' CIE2 releases (Comparison & Compliance and Enforcement), DVLA are not directly passing personal data to Experian. However, further details of MIB's system may be required, to confirm what data they will be sending to Experian when completing the daily insurance checks – these are made prior to the transmission of the 'Keeper Details Request' and 'Cases for Enforcement' files to DVLA.	H	L	L

* For each privacy risk there could be a number of options for avoiding or mitigating that risk. You should list all the options and then consider the residual risk for each one.

Stage 8 ► Approval

8.1 Recommendation

CIE has gone through a public consultation and an initial PIA was completed. A Memorandum of Understanding (MoU) covering the development project phase of CIE and a Service Level Agreement (SLA) is currently being drafted that will cover CIE operations once live including use and disclosure of data. CIE has the following governance a Project Board which meets monthly and is chaired by the Project Executive, Programme Board which is chaired by the Programme Manager and CIE Project Manager when needed and DfT Steering Group which is quarterly and the Project Executive and Project Manager attends. Therefore sign off of this PIA is recommended.

8.2 Approval

CIE2 Senior Responsible Owner – David Hancock

Signed copy on CIE registered file and with MIB

Stages 5 - 8 completed by:		Date:	21/1/10
----------------------------	--	-------	---------

Stage 9 ► Readiness for service

The project phases of CIE are governed by MoU's covering DVLA and MIB project teams. For the live operation of CIE a Service Level Agreement will be put in place and signed at Director level. The SLA will cover all aspects of CIE including the security and use of data. The SLA will be renewed annually.

Stage 9 completed by:		Date:	21/1/10
-----------------------	--	-------	---------

Stage 10 ► Review or audit

As part of PIA process all necessary parties have been consulted. Review will take place 6 months after go live.

Stage 10 completed by:		Date:	21/1/10
------------------------	--	-------	---------

DPA Compliance Check

	Question	Answer
1	What type of personal data is going to be processed?	Please see section 1.2.1
2	Which of the grounds in schedule 2 of the DPA will provide a legitimate basis for the processing?	Schedule 2 paragraph 5(c) - The processing is necessary for the exercise of any of the functions of the Crown, a Minister of the Crown or a government department OR Schedule 2 paragraph 6 - The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
3	<p>If sensitive personal data is going to be processed, which of the grounds in schedule 3 (in addition to the schedule 2 grounds) will provide a legitimate basis for that processing?</p> <p>Note – Sensitive personal data is personal data consisting of information as to (a) the racial or ethnic origin of the data subject, (b) their political opinions, (c) their religious beliefs, (d) whether they are a member of a Trade Union, (e) their physical or mental health, (f) their sexual life, (g) the commission or alleged commission by them of any offence and (h) any proceedings for any offence committed or alleged to have been committed by them.</p>	<p>Sensitive information will be shared in the CIE process under Schedule 3, conditions:</p> <p>6(a) necessary for the purpose of legal proceedings 7(a) for the exercise of any function conferred on any person by or under enactment and 7(c) the exercise of any function of the Crown, Minister of the Crown or government department.</p>
4	<p>Are there any special considerations relating to Article 8 of the Human Rights Act that will not be covered by the PIA?</p> <p>Note – This Article provides that everyone has the right to respect for his private and family life, his home and</p>	No

	correspondence. It is subject to qualifications relating to national security, crime etc.	
5	Will any of the personal data be processed under a duty of confidentiality? If yes, how is that confidentiality being maintained?	No
6	How are individuals being made aware of how their personal data will be used?	Individuals will be informed of the CIE process and change in legislation via an education and publicity campaign through direct gov and leaflets.
7	Does the project involve the use of existing personal data for new purposes?	Yes, CIE project will bring together DVLA's Vehicle database and MIB Motor insurance database together for the purpose of identifying, advising then prosecuting uninsured drivers
8	What procedures will be in place for checking that the data collection procedures are adequate, relevant and not excessive in relation to the purpose for which the data will be processed?	CIE and MIB will be subject to audit checks which will assure that the procedures in place for checking that the data collection procedures are adequate, relevant and not excessive.
9	How will the personal data be checked for accuracy?	Please see sections 1.2.2/3
10	Has the personal data been evaluated to determine whether its processing could cause damage or distress to data subjects?	The Insurance Advisory letter is the opportunity for an individual to update their record if they do receive a letter by mistake. Publicity will also emphasise the importance of updating your record.
11	Will there be set retention periods in place in relation to the storage of the personal data?	Yes, please see section 1.2.5
12	What technical and organisational security measures will be in place to prevent any unauthorised or unlawful processing of the personal data?	The Project has in place a Code of Connection document and a Service Level Agreement is being drafted which will detail the security measures in place to prevent any unauthorised or unlawful processing of personal data which both DVLA and MIB will sign up to.
13	Will you be transferring personal data to a country outside of the European Economic Area? If so where, and what arrangements will be in place to ensure that there are adequate safeguards over the data?	No