Data Privacy Impact Assessments Guidance Note

What is a Data Privacy Impact Assessment?

Privacy Impact Assessments (DPIA) are a tool used to ensure risks to an individual's privacy are identified within new projects, policies and processes which involve the processing of personal information. Privacy intrusion can be physical in nature – images captured on CCTV or ANPR systems or biometric data collected as a result of drug and alcohol testing for example. It can also be informational – the content of emails and other forms of correspondence or the monitoring of telephone calls for example.

For a DPIA to be effective it must be undertaken at the start of a project allowing problems to be identified and subsequently addressed at an early stage. The DPIA template can be found at Annex A.

Off-setting privacy risks carries the additional benefits of reducing costs and damage to Highways England's reputation by decreasing the risk of security breaches and ensuring compliance with the General Data Protection Regulations (GDPR).

Identifying privacy risks

A project can impact on privacy in a variety of ways. Privacy risks to individuals often carry associated compliance and organisational risks. For example a project perceived as intrusive or insecure by our customers and stakeholders also increases the risk of fines, reputational damage and ultimately the failure of the project.

The DPIA should therefore identify privacy risks to individuals, corporate risks such as fines for non-compliance with the GDPR or reputational damage and compliance risks.

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge
- New surveillance methods may be an unjustified intrusion on their privacy
- Measures taken against individuals as a result of collecting information about them may be seen as intrusive
- The sharing and merging of datasets can allow the collection of a much wider set of information than individuals might expect
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information
- Collecting information and linking identifiers may mean that information is no longer safely anonymised
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk

- If retention periods are not established information may be used for longer than necessary

Corporate Risks

- Non-compliance with the GDPR or other legislation can lead to sanctions, fines and reputational damage
- Problems which are only identified after the project has launched are more likely to require expensive fixes
- The use of biometric information or potentially intrusive tracking/monitoring technologies may cause increased concern and cause people to avoid engaging with the company
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business
- Public distrust about how information is used can damage the company's reputation
- Data losses which damage individuals could lead to claims for compensation

Compliance Risks

- Non-compliance with the GDPR
- Non-compliance with sector specific legislation or standards
- Non-compliance with human rights legislation

Examples of projects which require a DPIA

The core principles of a DPIA can be applied to any project which involves the use of personal information, or to any other activity which could impact on the privacy of individuals.

A DPIA should be conducted for a variety of projects including:

- A new IT system for storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A proposal to identify people in a particular group or demographic and initiate a course of action
- Using existing data for a new and unexpected or more intrusive purpose
- A new surveillance system (especially one which monitors staff and/or members of the public) or the application of new technology to an existing system (adding automatic number plate recognition capabilities to existing systems for example)
- A new database which consolidates information held by separate parts of an organisation
- Off-shoring of systems (including cloud-based systems) which hold personal information

Responsibility for conducting a DPIA

The Data Protection Officer can coordinate and advise on the DPIA process although input from those with knowledge of and responsibility for projects (project managers and sponsors for example) will be also be required.

Consultation with internal and/or external stakeholders can highlight privacy risks based on additional areas expertise and interest and should therefore also be considered.

Identifying privacy risks and evaluating solutions

- Identify each privacy risk and devise a solution to reduce, eliminate or accept those risks – most projects will require the acceptance of a degree of risk, the decision must therefore be based upon whether the impact on privacy is proportionate to the aims of the project
- Assess the costs and benefits of each approach, looking at the impact on privacy and the effect on the project outcomes
- Integrate the DPIA outcomes back into the project

Recording outcomes, sign off and publication

- Produce a DPIA report detailing the issues, risks and solutions
- Obtain signoff – the DPIA should be approved at a level appropriate to the project
- Consideration should be given to publishing the report (or a summary) which improves transparency by informing relevant stakeholders

The Data Protection Officer dataprotectionadvice@highwaysengland.co.uk can provide further advice and guidance relating to DPIAs. Additional information can also be found on the Information Commissioner's Office website: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Highways England Passport Scheme Data Privacy Impact Assessment

Step one: Identify the need for a DPIA
Explain what the project aims to achieve, what the benefits will be to: the company, individuals and other parties. It can be helpful to link to other relevant documents related to the project, a project proposal for example. Summarise why the need for a PIA was identified

Background

The Highways England (HE) Passport scheme uses a smartcard which holds information relevant to a person's "Authority to Work" on construction and operational sites involving the Highways England supply chain. The scheme is currently in a proof of concept stage (from November 2017 to end of October 2019) to enable thorough testing of its use from a technical and operational point of view

The card holds data that can be checked using a Smartphone or a card reader to confirm a person's identity, qualifications and work competences, training, and work patterns. Its purpose is to improve the safety environment for those working for Highways England and its supply chain it is jointly owned by Highways England and its supply chain and is currently governed through a Steering Group that meets monthly.

The scheme also involves a Common Induction training course that all Cardholders need to attend before they can use their cards. This will eventually produce a cost saving for the supply chain by not having to repeat company specific inductions for sub-contractors or staff from other companies working on their site.

Passport uses the software system developed by Reference Point and supported by Mitie who operate the system for Highways England on behalf of the supply chain during the "proof of concept".

Eventually each card may hold data on Drug and Alcohol testing results however a decision to do so will be considered as part of the proof of concept – this data is not currently collected.

The requirement for a privacy impact assessment was identified through discussions with Highways England's Passport Scheme project team, Legal Counsel and Data Protection Officer regarding risks of Highways England assuming the role of Data Controller for the Passport Scheme.

Step two: Describe the information flows
The collection, use and deletion of personal data should be described here (it may be useful to refer to a flow diagram for example). Where possible the number of individuals likely to be affected by the project should also be recorded.

Details of each cardholder (a Person record) are entered into the Mitie data entry page

by a “Passport Administrator” (or if the person requiring a smartcard does not have an administrator these details are entered by Mitie). Mandatory information required is name and (as a unique identifier) National insurance Number. A photograph is also required. Mitie then produce the Smartcard which contains this information and the competences and qualifications of the individual concerned This information is readable from a Smartphone (with the appropriate App downloaded onto it) or card reader. The card is then posted to the individual via their administrator or direct from Mitie. The data can be accessed by any administrator. It is stored in the UK.

Data relating to administrators is stored and processed to ensure relevant controls are in place so that access to workforce data can be restricted to only those individuals (administrators) with a legitimate need to view/process this data, and so that an audit history of changes to data made by administrators can be maintained.

Data relating to individual workers is stored and processed to allow Highways England and its supply chain to ascertain the identity of individuals and ensure that they have the appropriate pre-requisites to complete work on behalf of the Client/contractor (ie appropriate competences and/or training).

The administrator places on the card competences or training carried out by the cardholder.

The approximate number of individuals likely to be affected by the project is up to 55,000. This represents the upper end estimate of the total Highways England supply chain and the total number of Highways England employees (although it is doubtful whether more than half of the approximate 5000 HE employees would require a Passport Smartcard).

Consultation requirements

Explain what practical steps will be taken to ensure privacy risks are identified and addressed. Who should be consulted, internally and externally? How will the consultation be carried out? This should be linked to the relevant stages of the project management process. Consultation can be used at any stage of the PIA process.

A time bound consultation exercise has not been carried out however discussions on privacy risks have taken place with supply chain through the Passport Steering Group that meets monthly. Also the “proof of concept“ itself is to identify technical and operational issues, including issues around GRPR and privacy.

Step three: identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

Privacy issue	**Risk to individuals**	**Compliance risk**
Smartcard is lost or stolen	***Personal data is accessed***	Breach of Article 5 1(f)
Data breach at Mitie via IT systems.	***Personal data is accessed***	Breach of Article 5 1(f)

Data breach in one of the supply chain via IT systems	***Personal data is accessed by unauthorised persons***	Breach of Article 5 1(f)
Data breach at Highways England via IT systems	***Personal data is accessed by unauthorised persons***	Breach of Article 5 1(f)
Need for Privacy Statement	***Data subjects don't know how their information is going to be fairly treated***	*Breach of Article 5 1(a)* *Breach of Article 6 1(e)* *Breach of Article 9 2(g)*

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result** *is the risk eliminated, reduced, or accepted?*	**Evaluation:** *is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?*
Risk of access to personal data via data breach at either Mitie, Highways England or in the Supply Chain.	Secure systems and processes are in place. These include clear instructions to Passport Administrators about the handling of personal data and only those who need access to data have that access.	Reduced (no system can be 100% secure)	We are compliant with relevant article
Risk of access to personal data via stolen or lost smartcard	Only a subjects Title, first and surnames and photo are held electronically on the Smartcard (this information is also printed on the card itself). The only other electronic data is information regarding current competences, employment and	Reduced (no system can be 100% secure)	We are compliant with relevant article

	previous 24 hours of card swipes. Cardholders are reminded of the need to keep their card secure.		
Need for Privacy Statement	Produce Privacy Statement	Eliminated	We are complaint with relevant Articles

Step five: Sign off and record the DPIA outcomes
Who has approved the privacy risks involved in the project?
What solutions need to be implemented?

Risk	Approved solution	Approved by
Risk of access to personal data via data breach at either Mitie, Highways England or in the Supply Chain.	Secure Systems and Processes	**Ian Moreton** **Project Director** **Date:**
Risk of access to personal data via stolen or lost smartcard	Limited electronic data available on Smartcard	**Ian Moreton** **Project Director** **Date:**
Need for Privacy Statement	Production of Privacy Statement	**Ian Moreton** **Project Director** **Date:**

Step six: Integrate the DPIA outcomes into the project
Who is responsible for integrating the DPIA outcomes into project plan?
Who is responsible for implementing the solutions that have been approved?
Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Risk of access to personal data via data breach at either Mitie, Highways England or in the Supply Chain.	Already completed on set up of Mitie system for HE Passport Scheme	**Andrew Page-Dove** **SRO** **Date:**

Risk of access to personal data via stolen or lost smartcard	Already completed on set up of Mitie system for HE Passport Scheme	 **Andrew Page-Dove** **SRO** **Date:**
Need for Privacy Statement	Uploaded to Privacy Policy link in the Highways England Passport Home/Login page on 12 June 2018	 **Andrew Page-Dove** **SRO** **Date:**

Contact point for future privacy concerns Graham Woodhouse Data Protection Officer