DPIA - St Martins Housing Trust
Driving Record Insurance Check

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	St Martins
Title of DPO	System Data Coordinator
Name of controller contact	Head of Finance

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
At St Martins we use an Excel spreadsheet named 'Driving Record Insurance Check' (which is password protected and kept in a restricted folder) and electronically scanned documents kept in personal files to record information about the driving licence record of St Martins staff who may drive St Martins fleet vehicles. This personal information includes NI number, driving licence information (name, address, driving number) and driving record information (offence codes, penalty points). We believe that this DPIA is required because, in the event of a data breach, the data recorded in this system could compromise individuals' health & safety, and leave them vulnerable to identity theft.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Driving licence data, NI number, and consent to process is gathered from staff by e-mail and/or face to face. St Martins obtains driving record information from the www.gov.uk website. The data comprises:

Offence codes
Penalty points
Renewal dates

Offence codes and number of penalty points (but not name or other identifiable items) may be discussed with St Martins insurers if the number of offences/points is high. This is to clarify whether such an individual can be covered by the insurance policy. Individuals are informed if they cannot be covered and are therefore not permitted to drive fleet vehicles.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The nature of the data is described at section 2 above. Special category data is not included. Criminal offence data can sometimes be included (because serious driving offences, such as drink driving, drug driving, dangerous driving etc, constitute criminal offences and form part of the criminal record). Our condition (from Schedule 1 of the DPA 2018) for the processing of criminal offence data is 'insurance'.

The amount of data stored is kept to the minimum required to successfully manage the Driving Record Insurance Check process. The checks are conducted as required and periodically reviewed/repeated.

Driving record data will be retained for the duration of staff employment plus one year after, subject to any minimum statutory requirements for particular records.

The current number of staff who drive fleet vehicles is approximately 40, all working in the general Norwich and Norfolk area.

Regarding data minimisation and the identification & deletion of records which are older than our agreed retention period. As part of the annual review of this DPIA, the owner of this business process will consider the ongoing need to create a process (manual or automatic) which covers both electronic and paper records.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
St Martins relationship with staff is employer/ employee in nature All data subjects are able to review the data being held for accuracy. People from vulnerable groups (not children) may be among St Martins staff at any time. This type of processing is well established in the employer/employee arena and is not novel. St Martins is accredited to the NHS Data Security and Protection Toolkit (DSPT) at the level 'standards met'. St Martins has Cyber Essentials accreditation, which defends against common threats to cyber security. St Martins has an internal IT Technician (with access to further support from Cube Connection if required) to maintain all computer systems, hardware and software. All St Martins staff have completed Data Security Awareness training.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
The purpose of our processing is to ensure appropriate insurance cover for St Martins fleet vehicle drivers. The intended effect on staff is that they will be reassured that insurance cover is appropriate. The benefit for St Martins is that our fleet insurance cannot be invalidated. More broad benefit is that all other road users are reassured that all St Martins drivers have appropriate insurance cover.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
All data subjects provide their consent and are able to review the data being held for accuracy. St Martins insurers have stipulated the need for this process and the www.gov.uk website provides the required driving offence data. This supports the view that further consultation is not required. IT support, provided by an internal IT Technician (and Cube Connection if required), ensures St Martins has the best cyber security at all times. St Martins is accredited to the NHS Data Security and Protection Toolkit (DSPT) at the level 'standards met'. St Martins also has Cyber Essentials accreditation, which defends against common threats to cyber security.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Our lawful basis for processing is 'legal obligation' as the personal data must be processed to comply with a common law or statutory obligation. Our condition (from Schedule 1 of the DPA 2018) for the processing of criminal offence data is 'insurance'. Our processing achieves its purpose, as we now have driving record data for all drivers of fleet vehicles. All staff are able to review their driving record data for accuracy. No international transfers of data are made.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1) Staff are distracted/called away from their computers without locking them, meaning unauthorized people could access data.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
2) Passwords are guessed or shared meaning unauthorized people could access data.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
3) Information is recorded inappropriately generating inaccurate data.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
4) Cyber attack allowing access by unauthorized people.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
1)	Regular staff training and frequent reminders of the dangers of leaving computers unlocked and unattended.	Eliminated reduced accepted	Low medium high	Yes/no
2)	Frequent reminders to use passwords which are unrelated, cannot be guessed and not to be shared.	Eliminated reduced accepted	Low medium high	Yes/no
3)	User training in, and familiarity with, data protection principles and St Martins policies. Data is double-checked by a second team member.	Eliminated reduced accepted	Low medium high	Yes/no
4)	Continued commitment to maintaining Cyber Essentials accreditation.	Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item v2.0	**Name/position/date**	**Notes**
Measures approved by:	Head of Finance	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Head of Finance	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	System Data Coordinator	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comment: Version 2.0 includes a reminder to consider if there is a need to identify & delete records which are older than agreed retention period (at Step 2 'Describe the scope of the processing').		
Consultation responses reviewed by:	Head of Finance	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Head of Finance	The DPO should also review ongoing compliance with DPIA