DPIA - St Martins Housing Trust Under 1 Roof sign-in system

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
Subject/title of DPO	System Data Coordinator
Name of controller contact	Head of Community Services

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 Under 1 Roof facility we use a sign-in system named 'Registrar' to process information about the staff, clients and others who visit the facility. This information includes name, e-mail address (for staff only) and purpose of visit. 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?

Data is input in person by staff, clients and other visitors. The data includes:

- name
- e-mail address (for staff only)
- purpose of visit

The processing makes a record of attendances at Under 1 Roof for the purposes of security and health & safety.

Data is shared with software provider Genee to facilitate their support of the system.

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.

The amount of data stored is kept to the minimum required to successfully manage and process the Registrar system. It is used every day that Under 1 Roof is open.

Personal data will be retained for 1 year.

Current Under 1 Roof visitor numbers are approximately 125 per week.

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 Under 1 Roof users is facility-user/provider in nature, including staff, clients and other visitors.

Facility users provide their own data to begin with and may review that data at any time by request.

People from vulnerable groups (not children) may be among Under 1 Roof users at any time. This type of processing is well established in the facility-user/provider 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 that Under 1 Roof is a secure facility to visit.

The intended effect on users is that they will feel secure when visiting the facility.

The benefits for St Martins are reliable information for emergency evacuations, and that users/visitors who feel secure will visit again.

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 users are able to review their data held on Registrar for accuracy by request. 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 'legitimate interests'. It is necessary in order to provide a secure environment for Under 1 Roof users and visitors. We have conducted a Legitimate Interests Assessment (LIA) to ensure we can justify our decision. Our processing achieves its purpose, as evidenced by continued popularity of the facility and services. All users are able to review their data held on Registrar for accuracy by request. 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) When viewing reports, staff are distracted/called away from computer without locking, 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
1) Information is recorded inappropriately (by visitors) generating inaccurate data.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
2) 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**

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Head of Community Services, 13/12/22	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Head of Community Services, 13/12/22	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	System Data Coordinator, 13/12/22	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Draft DPIA provided, discussed, amended and agreed.		
DPO advice accepted or overruled by:	Head of Community Services, 13/12/22	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	Head of Community Services, 13/12/22	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	System Data Coordinator and Senior Management Team.	The DPO should also review ongoing compliance with DPIA