DPIA - St Martins Housing Trust Online Shop

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	System Data Coordinator
Name of controller contact	Head of Communications and Marketing

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 a computer system named Wordpress (and Woocommerce their ecommerce solution), accessible to customers via our website to process information about Online Shop purchase transactions and the people making them. Payment data is processed by Stripe and appears on St Martins bank statement. Online Shop allows us to manage personal data in order to best support customers by processing orders quickly and efficiently. This includes an automatic e-mail order confirmation and a Marketing department order fulfillment e-mail. Online Shop data includes personal information such as name, address, telephone number and e-mail address. Online Shop offers both physical and virtual products including mugs, calendars, event tickets and downloads. 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 about Online Shop customers is gathered by Wordpress (customer and order data used to fulfil the order) and by Stripe (financial transaction). The data includes:

- Full name
- Address
- Telephone number
- e-mail
- Thank you letters
- Reports
- Order values (received via Stripe and bank statements)

Data is shared routinely with auditors.

Data is kept in Wordpress for three years, after which it is manually deleted.

All data in the Wordpress system is hosted by Candour. The website is backed up twice daily and the backups are stored for six months, as part of the ongoing hosting package.

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. No special category data or criminal offence data is included. The amount of data stored is kept to the minimum required to successfully manage and process the Online Shop system. The frequency is dictated by the timing of orders, which can arrive daily. Customer purchase/order data is kept for three years, after which it is manually deleted. St Martins has approximately 100 Online Shop orders per year, mostly from the Norwich and Norfolk area but including some wider and even internationally too. Order data is recorded on Wordpress and Stripe for each order transaction. 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 data owners is charity/customer in nature. Customers entrust us with their personal data. Loss of control might be possible in the event of a data breach which is why we mitigate the risks (steps 4 and 5 below). People from vulnerable groups may be among customers at any time, but St Martins does not have this information. This type of processing is well established in the charity/customer 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 raise funds by selling products. The intended effect on customers is that they will feel valued and secure and will buy again. The benefit for St Martins is that customers who feel valued and secure will buy again and again. The benefit for the people supported by St Martins is that revenue helps fund our continuing services.

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?
Consultation with stakeholders during the project, included St Martins staff and the Digidodaa consultancy company. 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 'contract', because an online purchase constitutes a contract with the individual, and we need to process their personal data to comply with our contractual obligations including the fulfilment of the order. There is compelling justification for this processing as we believe there is no other way to achieve this purpose. Our processing achieves its purpose, as evidenced by a very low level of complaints. 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**

Step 7: Sign off and record outcomes

Item: v1.0	**Name/position/date**	**Notes**
Measures approved by:	Head of Comms & Marketing, April 2024.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Head of Comms & Marketing, April 2024	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	System Data Coordinator, April 2024	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
Comments: Comment: Version 3.0 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 Comms & Marketing, April 2024	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Head of Comms & Marketing	The DPO should also review ongoing compliance with DPIA