DPIA - St Martins Housing Trust Donations

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 'Beacon' to process information about the donations we receive and the people who make them (including fundraising volunteers who donate their time) either by direct debit, online via other companies, by post or by visiting one of St Martins' offices. In addition, spreadsheets are used to pass data about bank receipts between departments within St Martins. Beacon allows us to manage donor and donation data in order to best support donors and to process donations quickly and efficiently, including the sending of acknowledgement letters. Beacon data includes donor personal information such as name, address, telephone number and e-mail address and, where relevant, business information including business I.D. 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 donors and donations is gathered from bank statements for standing orders and direct debits (via Just Giving, Stripe, Virgin Money Giving, Go Cardless etc) for online donations, from funeral directors who administer donations in memoriam, and from personal callers to St Martins by staff using paper forms which are added manually into Beacon by Reception staff. St Martins uses this data to create reports and thank you letters, and to update the general ledger where necessary. Bank statement data is used to create spreadsheets which are in turn used to pass donation data from Finance to Fundraising within St Martins. A Beacon report is used to pass information about cash-in-person donations to Finance. The data includes:

- Full name
- Address
- Telephone number
- e-mail
- Thank you letters
- Reports
- Donation amounts received

Data is shared routinely with auditors.

Data is kept in Beacon for as long as the donor is active, after which it is identified by a system report, marked as 'archive' and manually deleted.

Data concerning fundraising volunteers is also recorded in a in a web-based system called 'volunteer signup' to manage street collections

All data in the Beacon system is automatically backed-up on a daily basis using Amazon servers in London.

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 donations system. The frequency is dictated by the timing of donations, which can arrive daily. Donor data is kept for as long as the donor is active (defined as 5 years after last contact, based upon GiftAid's 4-year authorization + 1 year), after which it is identified by a system report, marked as 'archive' and then manually deleted St Martins has approximately 3000 active donor records per year, mostly from the Norwich and Norfolk area but including some wider and even internationally too. Donation data is recorded on Beacon beginning when the first donation is received.

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/donor in nature. Donors 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 donors at any time, but St Martins does not have this information. This type of processing is well established in the charity/donor 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 attract, receive and process donations effectively and efficiently. The intended effect on donors is that they will feel informed, valued and secure and will donate again. The benefit for St Martins is that donors who feel informed, valued and secure will donate again and again. The benefit for the people supported by St Martins is that donations help 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 trustees, St Martins staff in Reception, Finance and Marketing, and a Beacon software 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 'legitimate interest'. This is appropriate as St Martins uses people's data in ways they would reasonably expect and which have a minimal privacy impact. There is also a compelling justification for the processing as we believe there is no other way to achieve this purpose. A Legitimate Interests Assessment (LIA) is reviewed annually. Our processing achieves its purpose, as evidenced by a high rate of repeat donations and 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**
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
4)	Continued commitment to maintaining Cyber Essentials accreditation.	Eliminated **reduced** accepted	**Low** medium high	**Yes**/no

Step 7: Sign off and record outcomes

Item: v1.0	**Name/position/date**	**Notes**
Measures approved by:	Head of Comms & Marketing 01/8/2023.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Head of Comms & Marketing, 01/8/2023.	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	System/Data Coordinator, 01/8/2023.	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:		
Consultation responses reviewed by:	Head of Comms & Marketing	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