DPIA – St Martins Housing Trust Purchase Ledger

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 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 YOOZ document management system and Sage Intacct to capture and process our purchase ledger information. Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders where they are individually identifiable and the information relates to them as an individual does constitute personal data. This includes personal information such as name, address, telephone, account data, customer/supplier number, and related data and correspondence. We believe that this DPIA is required because, in the event of a data breach, the data recorded in this system could compromise an individual's 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?

Supplier data is gathered from invoices after trading begins. An 'Authorised Supplier Request Form' is completed by the department manager and submitted to Accounts Assistant for approval when the supplier is added to Sage Intacct. Invoice data is captured using the YOOZ document management system and then transferred into Sage Intacct when St Martins processes the data. The data includes:

- Name of supplier
- Address
- Telephone number
- e-mail
- bank details
- payment value
- payment due date

Data is shared annually with auditors for St Martins.

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 Sage Intacct system. The processing frequency is weekly. All inputs and calculations are double checked for accuracy each week by a second member of staff. Purchase Ledger data is retained for the current tax-year +6, subject to any minimum statutory requirements for particular records. Records for current year + 2 are kept on-site at Head Office. 3 earlier years are kept off-site by our independent document management service, 'Closed'. Invoice transaction numbers are approximately 50 per week, mostly in the general Norwich and Norfolk area. Information is recorded on Sage Intacct and YOOZ (and earlier using paper records) from when the first purchase transaction is begun. Regarding data minimization 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 suppliers is supplier/customer in nature. All suppliers are able to review their data held on the Purchase Ledger system upon request. People from vulnerable groups (not children) may be among St Martins suppliers at any time. This type of processing is well established in the Purchase Ledger 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 Purchase Ledger processing is to validate invoices, to pay them accurately and on time, and create transactions in the accounts ledger. The intended effect on suppliers is that invoice processing will be accurate, on-time and query free. The benefit for St Martins is that the payments are made efficiently and on time.

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 suppliers are able to review the data held about them on request. Purchase Ledger is overseen annually by St Martins' auditors. St Martins staff operating the purchase ledger have completed Data Security Awareness training. 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'. It is necessary for the performance of a contract with the supplier, and to take steps preparatory to such a contract. Our processing achieves its purpose, as evidenced by a low rate of payment queries. Purchase Ledger data quality is checked monthly for quality and minimization. Purchase Ledger data is audited annually. All suppliers are able to review their data upon 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) 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

Step 7: Sign off and record outcomes

Item: v3.0	**Name/position/date**	**Notes**
Measures approved by:	Head of Finance, April 2024	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Head of Finance, 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: V3.0 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') AND new systems 'YOOZ' and 'Sage Intacct'.		
Consultation responses reviewed by:	Head of Finance - 20/02/24	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