DPIA – St Martins Housing Trust Payroll

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 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 Sage payroll to process information about the staff we employ in our Head Office, in our Outreach service, and in our accommodation projects and care homes. This includes personal information such as name, address, tax code, NI number, rate of pay and related correspondence. We use a spreadsheet-based Excel spreadsheet system to capture 'timesheet' attendance and absence information. We also share some staff personal data with Blackhawk Network, which operates Cyclescheme and Techscheme (which helps staff to purchase bicycle and IT equipment) on our behalf. We believe that this DPIA is required because, in the event of a data breach, the data recorded in these systems 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 gathered from staff using paper forms when they join St Martins and again whenever it changes. Attendance and absence data is captured using the Timesheet spreadsheet system. HMRC also provides tax information. St Martins creates more information (payslips, P60s, letters etc) during the course of the employment. The data includes:

- Full name
- Address
- Telephone numbers
- Personal e-mail
- Gender
- Emergency contact
- Tax code
- Tax YTD values
- Financial, payroll and tax information inc: salary, benefits, pension, bank account details, tax codes and values, NI category, NI codes and values.
- Annual leave, other leave and sickness absence records containing special categories of personal data inc: information about medical conditions, medical reports, reasons for sickness absence, reasonable adjustments and related correspondence.
- Termination of employment documentation inc: settlement agreements.

Data is shared routinely with HMRC, pension provider, auditors and Blackhawk Network (for Cyclescheme and Techscheme).

Payroll data will retained for the current tax-year +6, subject to any minimum statutory requirements for particular records, and then removed/deleted.

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 included. The amount of data stored is kept to the minimum required to successfully manage and process the Sage system. The frequency is dictated by the monthly payroll cycle. Payroll data will retained for the current tax-year +6, subject to any minimum statutory requirements for particular records. Current staff numbers are approximately 190, all working in the general Norwich and Norfolk area. Information is logged on Sage from when the offer of employment is accepted. 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, selecting the right staff to work here and then to manage and remunerate them appropriately. All staff are able to review their data held on the HR system (Open HR) and their payslip data 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 provide accurate and timely salary payments to St Martins staff. The intended effect on staff is that they will feel appreciated, valued and secure. The benefit for St Martins is that a workforce which feels valued and secure is a loyal workforce, with a low rate of employee turnover.

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 staff are able to review their data held on the HR system (Open HR) and their payslip data for accuracy. Sage payroll is overseen annually by an auditor. 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 data subject, or to take steps preparatory to such a contract. Our additional condition for processing special category data is 'health or social care'. Processing special category data is necessary to provide the best care and support, tailored to the needs and goals identified for and by the individual, and is conducted under the responsibility of CEO Dr Jan Sheldon who owes a duty of confidentiality under an enactment or rule of law. Our processing achieves its purpose, as evidenced by a low rate of payroll queries and a low rate of employee turnover. Sage payroll data quality is regulary checked for quality and minimization. Sage payroll is audited annually. All staff are able to review their data held on the HR system (Open HR) and their payslip 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

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: 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 Finance, April 2024	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