Appendix 3

CAMBRIDGESHIRE
& PETERBOROUGH
COMBINED AUTHORITY

# Data Protection Impact Assessments Guidance

| | |
|---|---|
| Type of document: | Guidance |
| Document produced by: | Cambridgeshire & Peterborough CA Data Protection Officer |
| Document approved by: | Cambridgeshire & Peterborough Combined Authority Board |
| Version : | Version 1 |
| Issue date: | |
| How is this shared? | Electronically |
| Date due for review: | Annually April |
| Reviewer: | Rochelle Tapping<br>Susan Hall |

| **Data Protection Contact** | | |
|---|---|---|
| **Contact Details** | **Email** | **Phone** |
| Rochelle Tapping | dpo@cambridgeshirepeterborough-ca.gov.uk | 07923250218 |

# Table of Contents

# Introduction

Data protection is all about using information about people responsibly and transparently. Every time we use a piece of information about someone then we will have an impact on their privacy. This is because the information we hold about them is personal to them so if we misuse or lose it then their private information could become public or we make decisions which affect their life.

When we start using new systems, collecting new information, or providing a new service then we will need to think about the impact on our customers' private life.

We need to think "Privacy By Design" which means we build protecting our customers' privacy into every project. It means we balance what we want to do against someone's right to privacy – what is good for us is not necessarily good for them. You can find out more about the idea of Privacy By Design later in this policy.

To help us to do all of this then we need to think about how we assess that impact; such as making sure that we have considered the risks of what we are planning, how we will reduce those risks and importantly is what we are doing fair. This is called a Data Protection Impact Assessment or DPIA for short.

# "If you only read this…"

Do make sure that you have completed a DPIA screening checklist before you start your project

Do explain clearly what the project is because not everyone is an expert in your area

Do make sure you confirm whether a DPIA is needed

Do make sure you know what the risks are and how you will mitigate them

Do ask the Data Protection Officer for advice and help

Don't think because we are commissioning a service that we are not responsible for the personal information

Don't think that this is for the Data Protection Officer to worry about, its your responsibility

# Who needs to do one?

Any one of us who is responsible for a project and/or managing a project needs to think about a DPIA. The project could be something brand new like a new service or new system or it could be changing a current service or system.

# What do I need to do?

The change in data protection legislation made it mandatory for us to consider the potential impact on privacy that the project or service could have. The first step is to complete a screening checklist so that the Data Protection Officer (DPO) can determine whether you need to do a further assessment.

# When do I need to do one?

You should do one at the start of the project or before you commission a service so that you have considered all the risks from the outset and can design processes that reduce or remove those risks.

# Quick Questions – and quick answers!

### We are just commissioning a service so we won't be collecting the information ourselves?

Maybe not but you are asking and paying someone else to do it on our behalf. They wouldn't do it if we weren't asking them to. This means that we have a responsibility for the use of that data.

### We are only getting anonymised data from the provider to help us review their performance.

See above answer – to give you that data, they need to have collected the actual personal information that we asked them to. We have a responsibility for it.

### The project involves many partners so who does this and do we need more than one?

No. The lead organisation needs to take ownership with the support of the other partners so there is just one DPIA but which covers all.

### If I need help then is there someone to help me?

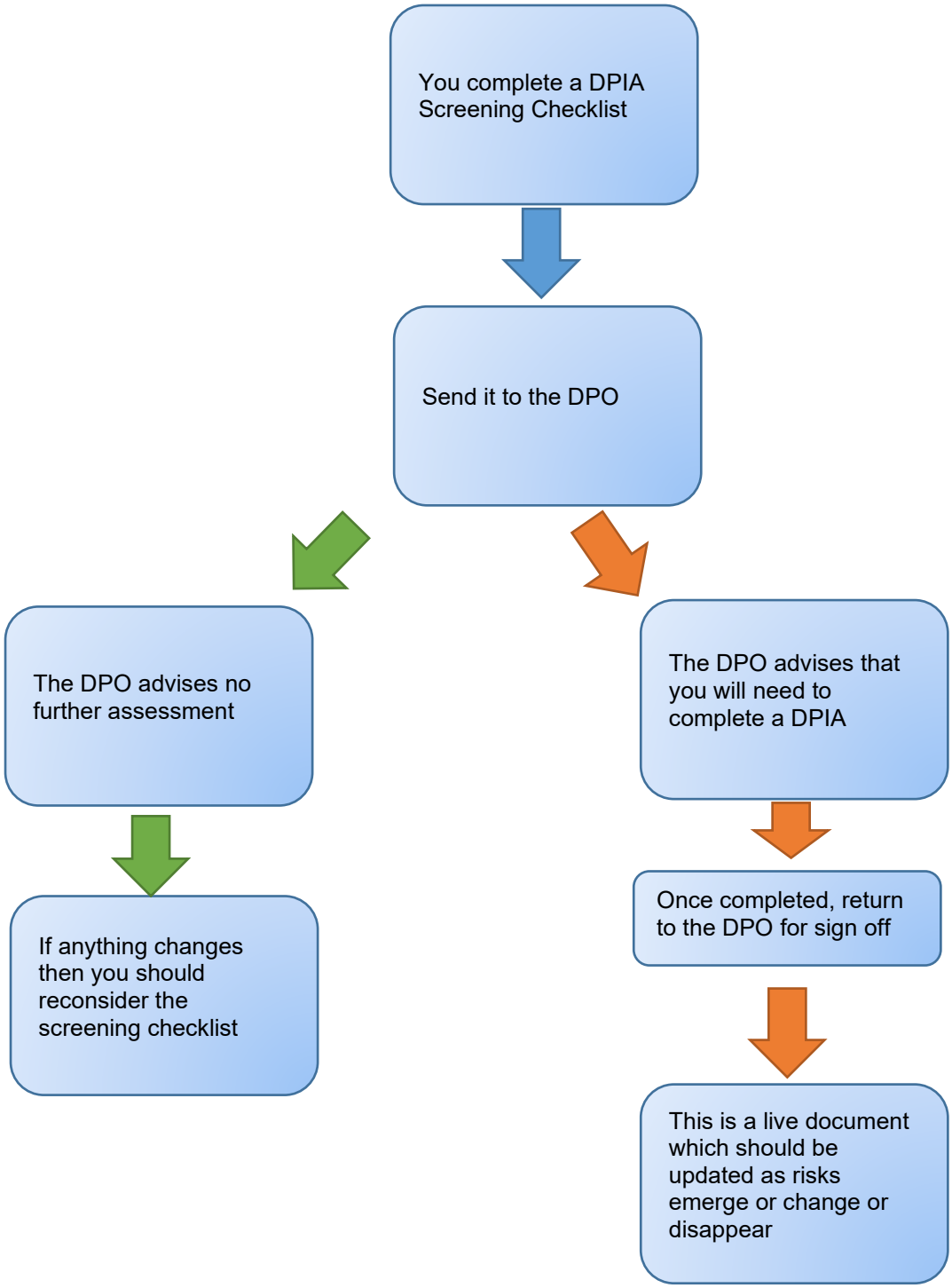
Yes the DPO is here for that. All we ask is that you explain in simple terms what your project is – what it is about, what information is being used, about who and why. Remember you are the person who knows the most about your service, not us.

### Is it a bit hard?

It may look like another bit of bureaucratic paperwork but actually it helps you understand what your risks may be beyond cost or deadlines. Knowing these and how you resolve them could help your project be even better.

# What is the process?

The flowchart below shows the outlined process and links to further sections.



# The Screening Checklist

This helps to show that you have considered privacy in your project. We need a clear and simple explanation of what your project is about. As well as the objective, we need you be clear on who is involved, what the benefits are and importantly what the risks are.

Remember we will not necessarily understand your service like you do so acronyms or abbreviations may not make sense.

## Data Protection

It is also at this stage that we ask you to consider what information you actually **need** to use and **not** what is easiest or **not** just what you want. Just because using the full data on 1000 people is easier than having that data anonymised or pseudonymised does not make it right. It may also help you avoid more paperwork!

### Minimised? Pseudonymised? Anonymised?

*Minimised* means that you have stripped back as much as you can. If you only need age and postcode then that is what you use rather than name, address and date of birth.

*Pseudonymised* means that we have replaced any data which could identify someone with a code known to us. So instead of John Smith we say Person 5TVRA. It means that we can look back and re-identify John Smith if we need to.

*Anonymised* information means that we will not be able to identify anyone even if we wanted to.

## Flows, Controllers, processors…

It is also here where we need to think if information is being shared between parties and why. This is important because along with why we have this project or why we have commissioned the service, then it helps determine who is a controller and who is a processor.

## Checklist Yes or No's

There are then a series of questions we need you to answer yes or no to. There are four situations where a DPIA is mandatory – regular profiling and automated decision making, using special category data on a large scale, undertaking regular monitoring of public space and high risk processing.

In the screening checklist, you will see how these are explained. Whilst the first three are each a question, the definition of high risk processing could be a number of factors.

There is a second category where a DPIA may not be required but could prove useful and helps understand the information we are collecting and the risks with it. There may be some discretion here as to whether a DPIA is done but remember the DPIA can be a very useful way of making sure that we have thought of all the possible risks and benefits to our service users. It shows that we have thought about our service users and their privacy.

# The DPIA

If a DPIA is required then we want this to be something that you can complete without it being too onerous or difficult.

The form covers a number of areas in more detail than the screening checklist but you can take some information from that to include in the DPIA.

## Project Information

This covers much of what was in the screening checklist but also identifies why a DPIA is being completed.

### Parties Involved

You should include all internal parties including the likes of Finance, Legal and ICT. Remember that all of these will have an input from costs to contracts to the system and its impact on the network.

It is also key to make sure that you have noted all external parties especially those who are acting on behalf of a party e.g. Serco acting on behalf of PCC or LGSS for CCC.

### Data Flow

This section is really important. This is where we identify where information is coming from and going to, what we are doing with it and why, who will have access and why, how we will protect it, where it will be stored and how long for.

### People

This is about the people whose data we are processing. We need to understand who they are, how we will explain what we are doing and how we make sure that we can meet their rights under data protection.

### Legal Basis

Anything we do with personal information must be lawful. This means that we have a reason to do something with that data and we can say what that is. There are six reasons for processing personal information and ten for processing special category data. We need to pick one of each.

### Risks

Whenever we process personal information, there will be risks and it is useful to identify those. Once we identify a risk then we need to say how we will mitigate or limit its impact and how we will know that this has been successful.

#### Unmitigated & High Risks

The assessment should highlight any risks we think we may encounter. It should also ensure that we have plans to reduce or eliminate those risks. If you believe that you have identified a risk which cannot be mitigated or even despite that mitigation remains high then speak to the DPO. We may have to discuss with the ICO if we want to go ahead with something which has such high risks.

# Who does what?

### All of us

We all need to think about a DPIA. We need to consider risks and how we mitigate them. Project managers and sponsors should ensure that a DPIA screening checklist is completed and any further assessments are also completed.

### Data Protection Officer

The DPO will assess the screening checklist and determine the next action – no further action or a DPIA. They are also there to advise you and challenge you in the nicest possible way. Their job is to help you consider risks, mitigation and compliance. They may discuss the matter with the Information Risk Group.

### SIRO

The SIRO is the senior officer with responsibility for security, risk and data. The SIRO will review and agree a full DPIA where necessary.

# Registers

The DPO will maintain a register of screening checklists and DPIAs. They will also ask services to consider what information needs to be added to the Information Asset Register.

# Monitoring and Review

There will be a quarterly report to the Data Protection Officer. This will inform training and risk assessments.

The Audit and Governance Committee receives 6 monthly reports on Information Governance. The report includes details of completed DPIAs.

This policy shall be reviewed annually after implementation.

.