Take your Data Protection Impact Assessment, (DPIA) to the next level, with these

DPIA TOP TIPS

DPIA

DPIAs are a really effective method of ensuring we're not collecting information that we don't need, (this is known as data minimisation) or using information unlawfully.

The DPIA form can look intimidating at first, but once you know what to do, it's as easy as pie. This handy guide should help support you and answer any questions that arise when completing your DPIA.

SEE THINGS FROM THE DATA SUBJECT'S PERSPECTIVE

When filling in your DPIA it might help to imagine that it's **your** data being processed.
You might ask:
Why are you doing this with my data?
Are you doing what you said you would?
Where can I find information about what you're planning to do with my data?
When did you tell me you were going to do this?
What measures are you taking to protect my data?
Try to keep these questions in mind when completing your DPIA.

EXPLAIN IN CONTEXT

The GDPR legislation puts the onus on us as the organisation to show our compliance with it, so when completing your DPIA, make sure the context is clear and you've explained in detail what all of the relevant parties will be doing and why.

For example, if an external partner is named in the DPIA, explain the capacity in which they're involved. Such as: Are they our contracted data processor? Are they simply receiving the data in their capacity as a legitimate data controller? Are there legitimate reasons for the collaboration?
If there's already a data processing contract in place, you could use the wording in Annex 1 of your contract.

ACBDTUSWTIFWYUTFTFT*

*Acronyms can be difficult to understand, so write them in full when you use them for the first time.

EXPLAIN EVERY STEP OF THE DATA'S JOURNEY

There's no such thing as too much detail, so be really clear when explaining the flow of data. Ask yourself:
Does your DPIA explain the full story of the data flow from the start to the end?
Are there any gaps?
Could you provide more detail?

PRIVACY NOTICES

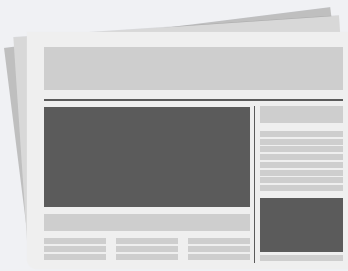
Privacy notices explain to individuals, (data subjects) what we're doing with their data. Therefore, it's important that you reference all of the relevant privacy notices that you will use to legitimise the use of their personal data, and check that the individual's data is being used for the reasons they were originally given.

PROVE YOU'RE ADHERING TO RETENTION PERIODS

If retention periods are not adhered to, KCC is in breach of one of the key data protection principles.

We're required by law to adhere to retention periods, so when referencing the retention schedule in your DPIA, make sure you say the specific sections of KCC's retention schedule that are relevant to your data processing.
We need to be able to prove that we are adhering to the law, and not keeping data for longer than is absolutely necessary.
Be explicit about how long the data is kept for; whether the retention periods are being adhered to; how they are being adhered to; and how this can be tested.

READ THE DPIA POLICY AND GUIDANCE DOCUMENTS



Before you start filling in your DPIA form, make sure you've read the DPIA guidance. We've recently updated it, so you might find some extra advice on elements of the DPIA you've been struggling with.
By reading the literature and keeping it close at hand, you'll be making sure that KCC is GDPR compliant!

FOLLOW THE GUIDANCE IN THE DPIA FORM

You must justify everything in the DPIA form, and just as you must justify why you **are** doing something, you must also justify why you are **not!**

For example, the guidance relating to consultation with data subjects in the DPIA template : The Information Commissioner's Office (ICO), states that, *"the views of individuals should be sought unless there is good reason not to and in most cases it should be possible to consult individuals in some form. If it is decided that it is not appropriate to consult individuals then this should be recorded in this section with a clear explanation as to why and how it would undermine security or be disproportionate or impracticable or compromise commercial confidentiality".*

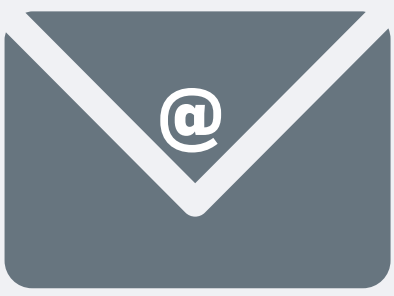
TRAINING

If you're going to be completing DPIAs regularly, why not speak to your manager to see if you can attend an external training course, such as those run by Act Now?
If you need extra advice on how to complete your DPIA, you should also take advantage of the DPIA drop in sessions that will be available soon.
Keep an eye on KNET to see when the drop in sessions are running.

INCLUDE KCC'S ORGANISATIONAL MEASURES

It is a KCC requirement that all staff have read, understood and followed KCC's Information Governance policies. The GDPR requires the inclusion of KCC's organisational measures. So it is important that you refer to all of these organisational measures; (from compulsory Information Governance training, to which of KCC's Information Governance policies are being used, and how).

For example, it isn't sufficient to simply mention the de-identification, pseudonymisation or anonymisation of data. Instead, you need to explain how the specific requirements in KCC's Anonymisation and Pseudonymisation policy are met, such as how the key to the pseudonymised data is kept secure.



GET IN TOUCH WITH US

If there's anything you're unsure of when filling out your DPIA, ask! We're here to help with any queries you have, and give you the support you need.
We also welcome any feedback that you have on ways to make the DPIA template more user friendly!
Just send an email to dpo@kent.gov.uk

WE'RE HERE TO HELP

Please don't take any comments on DPIA drafts personally. We're here to support you and protect you, by making sure that you're complying with the law every step of the way through your project.