DPIA CHECKLIST

A Data Protection Impact Assessment (DPIA) helps you identify and reduce risks to personal information. You must complete a DPIA if the processing is 'high risk' but you should consider carrying out a DPIA in any project involving personal data. Use this checklist to help guide you through the process.

DPIA AWARENESS

- [ ] All our staff know when we need to think about completing a DPIA when carrying out any project involving the use of personal data (whether it's a completely new project or where there's been a change to the nature, scope, context or purposes of our processing).
- [ ] We have a DPIA process.
- [ ] We have appropriate staff capable of completing the DPIA process and who have responsibility for this.
- [ ] Those who are responsible for the DPIA process have had the right training so they have all the necessary knowledge and skills.

INITIAL SCREENING

- [ ] I know that I must carry out a DPIA if we plan to do certain things with personal data in particular where there is going to be:
    - (a) a systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing, and on which decisions are based that produce legal effects concerning, or similarly significantly affecting, those persons;
    - (b) the processing of special category data on a large scale; or
    - (c) a systematic monitoring of a publicly accessible area on a large scale.
- [ ] I have checked if the processing is likely to result in a high risk to people's rights and freedoms (e.g. sensitive (special category) data, monitoring, profiling, using new technology, making automated decisions about people).
- [ ] I have asked my DPO (or person with responsibility for data protection) or the JOIC for advice if I am not sure.
- [ ] I have recorded my decision to do/not do a full DPIA.

I CAN DESCRIBE WHAT THE PROJECT IS ABOUT AND WHAT DATA I AM USING

- [ ] I have described what the project is and why we are doing it (the nature, scope, context and purposes of processing).
- [ ] I have listed the types of personal data we will be using (e.g. names, contact details, location, health information, financial data).
- [ ] I have identified whose personal data we are using (e.g. children, employees, vulnerable adults, service users, customers).
- [ ] I have explained how we will collect, use, store and share the data.
- [ ] I have identified and explained all the processes involved, including what third parties/software will be used.
- [ ] Where we are going to be involving third parties (including any data processors), I understand their own processes and data protection practices and what they will be doing with the data. I have explained the relationships using text and diagrams where appropriate).
- [ ] I have checked and recorded the lawful basis (Schedule 2 DPJL 2018) that we will be relying on to process the data (e.g. consent, legitimate interest, legal obligation).

WHO HAVE I SPOKEN TO?

- [ ] I have spoken to the right people about this project (e.g. IT, HR, legal, project managers) and I have recorded their information and views.
- [ ] I have thought about whether I need to consult anyone else such as the individuals who will be affected by the processing and where I have consulted them I have recorded their views.

DO I NEED TO USE THE DATA? IS IT JUSTIFIED?

- [ ] I have checked that the data we want to use is necessary for the project.
- [ ] I have thought about whether there is a less privacy intrusive way to achieve the same goal (can I achieve what I want to achieve, by more privacy friendly means).
- [ ] I have made sure that we will only be collecting and keeping the data that we actually need.
- [ ] I have made sure that access to the data will be limited to those who need it.
- [ ] I have set out how long we are going to keep the data for and explained what is going to happen to it when we don't need it anymore.

WHAT COULD GO WRONG?

- [ ] I have identified any risks to the rights and freedoms of individuals relating to our use of their data (e.g. what could happen if the data is lost or misused) .
- [ ] I understand and have set out what the potential harms could be (e.g. identity theft, financial loss, physical harm).
- [ ] I have thought about how likely it is that the risks and harms could arise and understand how serious the impact could be.

HOW WILL THE RISKS BE REMOVED/REDUCED?

- [ ] I understand and have clearly set out how we will keep the data safe and set out all the security measures that we will have in place (and which have been tested) (e.g. encryption, passwords, access limits, secure storage).
- [ ] I have set out how people can access their rights over their data (e.g. how they can access it, ask for wrong information to be corrected, ask for information to be deleted).
- [ ] I understand and have set out what will happen if something goes wrong and have set out a plan to deal with it (e.g. breach response).

COMPLIANCE WITH THE DPJL 2018

- [ ] I have made sure that the completed DPIA contains all the information required by Art.16(6) of the DPJL 2018.
- [ ] The DPIA is clearly written, in plain English and any technical terms used are clearly explained and defined (including using any diagrams).
- [ ] The DPIA has been reviewed and signed off by those with the appropriate seniority.
- [ ] A review date has been scheduled/included.

DO I NEED TO HAVE THE DPIA CHECKED BY THE JOIC?

- [ ] I have considered whether there are any risks I've identified that I have been able to remove, reduce or manage.
- [ ] If high risks remain, I have sent the DPIA to the JOIC either using their online form or in with all of the information required by Art.17(2) of the DPJL 2018.

MORE INFORMATION

Jersey Office of the Information Commissioner
2nd Floor
5 Castle Street
St Helier
Jersey JE2 3BT

Telephone number: +44 (0) 1534 716530
Email: enquiries@jerseyoic.org