Sample DPIA template

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	James Overbury
Subject/title of DPO	Deputy Clerk
Name of controller contact /DPO (delete as appropriate)	

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.

Framlingham Town Council conducted a survey in late 2019/early 2020 asking residents their views on a CCTV system. This was followed up by face to face interviews with businesses. 80% of residents and 31 out of 32 businesses called for a CCTV system to be installed.

The Town Council has an existing policy of the use of CCTV and its data and this has been extended to cover the town centre system.

The monitor for the cameras will remain off and not visible at all times unless images are being searched for as a result of a crime or an act of anti social behaviour. Only such images will then be shred with the police. The data is over written after seven days.

Proposal:
Framlingham Town Council agrees in principle to the introduction of public CCTV in Framlingham.
Purpose:
To deter criminal activity in Market Hill and its vicinity and provide evidence for the police in the event of offences being committed.
Evidence:
Crime figures for about the last three years for Market Hill and the surrounding area (Well Close to Saxmundham Road bordered by the Mere and Fore Street) were reviewed (see Appendix A).
Generally, the crimes recorded in this area make up about half the total for the town. The most prolific reported crimes are anti-social behaviour/public order, violent crimes and thefts. On average there is about one reported offence per week but there are instances of multiple offences on a single day.
The instances of criminal damage, burglary and anti-social behaviour focused on the town centre have drawn adverse comment and have caused concern for the community.
Public surveys:
The Town Survey indicated about 80% of responders in favour of CCTV.
A survey of businesses and residents in the vicinity of Market Hill showed 31 out of 33 responders in favour of CCTV.
Parameters of deployment:
Focussed on Market Hill with access/egress routes covered by cameras. The car parks in Fore Street and The Elms should be included in the coverage. This should maximise the opportunities to identify people committing offences in the Market Hill area.
Costs:
Two companies have previously been approached in relation to supplying CCTV for the Town.
Indicative cost for CCTV is likely to be in the region of £25k plus maintenance contracts at £600 - £2k per year. Both companies will be contacted to ensure that they are offering the same coverage, confirm the proposed operating systems and projected costs.

Source of funding:
If adopted, it is suggested that CIL funds are used for capital costs. There will be ongoing revenue costs for the Town Council.

Other considerations:
Any system adopted will have to be appropriate for a conservation area.
SCC will have to grant permission for the cameras to be mounted on their lamp posts.

Next steps:
If this proposal is agreed then the next steps will be to firm up the requirement, seek bids for the work and prepare a business case for FTC to consider.

Appendix A - Crimes recorded in the Market Hill Area 2017/20

Years	Total	Theft	Burglary	Violence	ASB/PO*	Criminal Damage	Vehicle Crime	Other Crimes
2017/8	54	11	7	10	10	4		12
2018/9	61	17	1	11	18	7	1	6
2019/20 up to Jan 20	36	9	1	11	12	1		2

*Anti-social Behaviour and Public Order offences.

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?
The data is captured by 17 cameras across the town, It is stored on a hard drive that is in a locked secure place within the Town Council Office. The images are only viewed by the Town Clerk (on in his absence the Deputy Clerk) and then only shared with the police. No one else has access to the images. It is under this system that data breaches and abuse are mitigated.

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 moving images captured by CCTV cameras across the town centre. The system is live 24/7 and recorded onto a secure hard drive and will be over written after seven days.

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)?
The relationship to those people whose images are captured by the cameras and the Town Council is one of location. The Town Council and the images are in the town of Framlingham. The Town Council is the only body that has the mandate to install the cameras and it is expected that this is understood. It is inevitable that children and vulnerable groups to have their images captured but the data will only be processed if they are seen by the images to have committed a crime or an act of anti social behaviour. The Town Council has a policy on the use of the system and its data and had made every effort to be compliant with all legislation and guidelines.

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 only time the data will be processed if it contains evidence of a crime or antisocial behaviour.

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?
Survey's have been conducted on the introduction of this system and they were very positive. Extensive research was undertaken and industry experts were consulted before the scheme was commissioned.

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?
The Town Council has a policy of the use of the cameras and its data. It is controlled by the Data Controller (Town Clerk). The process and policy will be reviewed annually. The only time the data will be processed will be to copy a short and directly relevant clip to a memory stick which will be then handed in person to a police officer. No other form of sharing or processing is allowed.

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**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Data is accessed and then abused by the one (or both) of the two people who hold the password to the hard drive.	Remote	Severe	Low
The office is broken into and the hard drive stolen	Possible	Severe	Medium

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**
		Eliminated reduced accepted	Low medium high	Yes/no
Abuse of Data	Minimum number of people have access to the data.	Reduction of potential abuse	Low	No
Theft of data	Data is locked away and password protected	Multiple barriers to accessing data	Medium	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		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:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

This DPIA will kept under review by:	James Overbury Town Clerk and DPO	The DPO should also review ongoing compliance with DPIA