Example of a completed Data Protection Impact Assessment form by Menter Môn

Menter Môn is a Social Enterprise that has installed public Wi-Fi systems in Anglesey and Gwynedd. These public Wi-Fi are used to collect anonymous footfall data that could support the town centres and high streets. Through a venture called Patrwm.io, Menter Môn made the aggregated data open-sourced to encourage towns to make use of this data and to see what patterns exist in each town. In developing Patrwm, a Data Protection Impact Assessment (DPIA) was completed to ensure compliancy.

Menter Môn want to share their DPIA with others who are considering using public Wi-Fi systems to monitor footfall analytics. However, it should be noted that this is to be **used solely as an example**. Each organisation must prepare their own DPIA. For more guidance on completing your own DPIA, please visit the Information Commissioner's Office's website: https://ico.org.uk. Furthermore a 'blank' DPIA template form can be downloaded via this link: DPIA template.

Using digital technology to gather intelligence can provide more insights and opportunities for towns in Wales, making them a SMART town. The 'Year of SMART Towns' project is a Welsh Government Funded project, delivered by Menter Môn. Through this project, Menter Môn hopes to encourage and facilitate towns to make best use of digital technology that can support data-driven decisions.

Contents

Data Protection Impact Assessment

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

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	
Subject/title of DPO	
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.
The Patrwm project aims to provide a wide range of data analytics services about town centres and other locations to the public, using data from Wi-Fi access points, and other sensors such as air quality, bins and weather. The system has not been designed to model or profile individuals themselves. It reports back on aggregated patterns of behaviour via interactive data visualisations. We determined that a DPIA was required due to the innovative nature of what the solution aims to deliver and because Patrwm was designed to systematically monitor publicly accessible places on a large scale;

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?

Footfall Data is collected via an encrypted API request from individual Wi-Fi access points every nn minutes. The only data that is retrieved is the device MAC address, time and data and access point ref. Any other data that might form part of Wi-Fi probe/announcement from a device i.e. device type, browser etc is not collected. stored or prcessed. In addition, for areas where the provision of an actual Wi-Fi service is not possible. Probe data is collected from secure LoRaWaN Wi-Fi sensors, this is collected and processed in exactly the same way.

The MAC address is then hashed using SHA1(or other) where the MAC address is already masked, a seed is inserted to ensure that any Hash enables the persistence of uniqueness.

Data from each hashed MAC address is then aggregated to display average dwell times and the number of unique visitors on that day. No processing is done to verify whether device has been in other locations (i.e. town centres) or over several days.

Information is presented to public on open access website via interactive visualisations of daily total numbers of devices, device dwell times and trends across towns/locations.

We did not identify MAC address data as being high risk because no other data sources are in use or available to Patrwm that might enable a link to be made between a MAC address and an individual. We did however consider that appropriate and reasonable actions should be taken in order to ensure that this data could not be used in conjunction with other data sources by hashing the mac addresses and ensuring that there was no API/endpoint in place for data to be extracted out of the Patrwm system.

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 specific solely to a Device Wi-Fi probe/announcement. Patrwm only works with a hashed set of data that is: Device Mac address Time and Date Access point/Sensor ID Town/Location ID The system is envisaged to be processing 10s of 1000s of records on a daily basis across 8 locations. Data retention period is no more than 3 yrs (in order to enable trend analysis i.e. to visualise holiday trends). We do not regard that any individual will be impacted. The system currently operates across Gwynedd and Anglesey, it is hoped that this will grow across Wales in the next 12-24 months. Patrwm does not include any special category or criminal offence data.

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)?
It is the opinion of the Controller that there is no relationship with any individual. If an individual does not want their device to be counted in a town centre or other location that has Patrwm they could put their device into flight mode, this would also apply in many other locations i.e. supermarkets, shopping centres, airports, stadia, conference centres and hotels. An individual's device (which is not already connected to Wi-Fi) is announcing itself on a frequent basis, the data from this announcement is being captured and logged by all nearby Wi-Fi Access Points whether private or owned by an organisation. We are sensitive to the concerns that MAC address data can to some individuals be regarded as being personal data. Although we do not agree with this, and in the absence of a definitive legal position this is why we specifically exclude any other data source / feed that could be used to identify an individual from their device's MAC address. This is why this data is hashed in order to ensure that it is de-personalised and that all functions of Patrwm are performed on the basis of aggregated NOT individual behaviours. The current state of technology means that the latest releases of Android, iOS, OSX and Windows 10 all set MAC address masking as standard feature. This means that the majority of devices are now masking and changing masking MAC address data on a daily basis.

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?
There is absolutely no intended effect on individuals. Patrwm is there to provide insight into aggregated behaviours in town centres in order to help high street businesses to be able to better measure the impact of any interventions i.e. changes to opening hours, marketing activities, events, Free Parking, environmental improvements. In addition, in conjunction with other sensor data feeds the aggregated patterns of activity in a location, combined with bin sensor data and weather datacan help service delivery managers to be informed of when a specific bin might need emptying in advance. Air quality sensor data can help clarify pollution or pollen issues in a locality helping individuals to make informed decisions on when might be best to visit the location. The broad benefits of the processing is to help people in town centre and other publicly locations make better informed decisions on the basis of aggregated data feed visualisations and trend analysis.

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?
We do not intend to seek individual's views. This is a ubiquitous technology. We have taken reasonable actions to ensure that device MAC address data is de-personalised, aggregated and is not used in conjunction with other personal data. We have asked Data Controllers of the project for their opinions.

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?
We are using publicly accessible data to provide insight (based on anonymised, secure and aggregated data) to town centre businesses, Local Authority Service delivery managers to improve quality of services. We are not aware of any other method that would provide the coverage and consistency. Beam breakers, manual counts are prohibitively expensive and extremely location specific. We have ensured data quality and minimisation by using SHA1/seed to 'de-personalise device mac address across both masked and unmasked MAC addresses and by only storing and processing device MAC address and time stamp/location. Any function creep that might imply that individual device addresses would be tracked or reported back on would require a new DPIA and full consultation with any relevant stakeholder in addition to the controller(s). We are not sure what or how we can provide any information back to individuals other than via a privacy statement on the Patrwm website i.e. there is no way that we could identify an individual even if they provided us with their device MAC address. Some Network hardware providers enable individuals to submit their Device MAC address and once approved, all network equipment that is in use will not 'see' this device. Patrwm does not run the Wi-Fi networks, nor the hardware. Patrwm data is stored and processed in the UK & IRL only.

Step 5: Identify and assess risk

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**
Patrwm data store is hacked and data stolen	Remote	Minimal	Low

Step 6: Identify measures to reduce risk

All data in Patrwm data store pertaining to a Wi-Fi probe is hashed.

We could consider removal of all/any de-personalised data records at the end of each monthly analysis, but this might cause issues with data accuracy/consistency on reporting over periods that cover a month end.

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

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:		The DPO should also review ongoing compliance with DPIA