South Somerset District Council

Date Protection Impact Assessment: Yeovil Alcohol Public Space Protection Order

Step 1: Identify the need for a DPIA

Explain broadly what the 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.

South Somerset District Council proposes to adopt two Public Space Protection Orders (PSPO) to restrict the consumption of alcohol and begging within the town centre of Yeovil. The enforcement of these PSPO will involve the collection and retention of evidence of any breeches. This evidence is likely to be personal and sensitive in nature and hence will be subject to data protection requirements.

Examples of the types of Special Category data includes:

- race
- ethnic origin

The default retention time of the data is 31 days.

A DPIA is therefore required.

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 another way of describing data flows. What types of processing identified as likely high risk are involved?

The PSPO allows an authorised person, such as the Compliance and Enforcement Specialist, Locality Officer or police officer to control the consumption of alcohol within the designated public place if they believe that someone is causing or likely to cause anti-social behaviour. If someone is consuming alcohol or intends to consume alcohol they can require them to stop or they can confiscate the alcohol.

- It is only if they fail to surrender the alcohol to an authorised officer or police officer do they commit an offence, breaching the PSPO.
- All incidents of alcohol being confiscated or disposed of to be reported for evidence purposes.

Enforcement of the Alcohol PSPO

The statutory guidance states that those found to be consuming alcohol within the area, against the terms of the order (causing or likely to cause Anti-Social Behaviour), are required to surrender any alcohol (sealed or unsealed) at the request of an authorised officer, be them a Police officer, PCSO or Local Authority officer. It is only if they fail to surrender the alcohol is an offence committed, breaching the PSPO.

Warning

Where any person is requested to desist from breaching a PSPO and immediately complies, the officer will verify the details of the person; name, address, date of birth and record the details on the appropriate police system and pass the information onto SSDC. A warning letter will then be sent to the person by SSDC. This information is not deemed to be Special Category data will be recorded on the Civica APP system.

Direct Breach

If somebody breaches the PSPO in not handing over the alcohol on request the police will complete a witness statement, supported by Body Worn Video evidence, giving the details of the offence, location, how they have breached the order. This video evidence is potentially personal and Special Category data.

Storing and Viewing a Recording

- The recordings will be stored on a secure Council computer drive.

- The recordings will only be accessible by authorised personnel and all non-evidential data will be maintained for a maximum of 31 days before it is deleted. Recordings required as evidence will be kept for a maximum of 6 months or until the evidence is no longer required, whichever is longer.

- Any evidential data will be deleted once it is no longer required. A record or audit trail of this process will also be captured.

- The recording will only be viewed by authorised personnel where evidence exists to support the Councils enforcement functions.

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 data collected will be in the form of audio/visual recordings. As such special category data is likely to be collected including:
    - race
    - ethnic origin
- Data is likely to be collected on an infrequent basis by police personal. The recordings will be stored on a secure Council computer drive.
- The recordings will only be accessible by authorised personnel, these being:
    - Compliance and Enforcement Specialist

  All non-evidential data will be maintained for a maximum of 31 days before it is deleted. Recordings required as evidence will be kept for a maximum of 6 months or until the evidence is no longer required, whichever is longer.
- It is currently unknown how many individuals will be affected but the number is likely to be small.
- Recordings are likely to take place only with the area defined by the PSPO.

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 Council officers will be dealing with enforcement scenarios. The purpose of passing on evidence is to provide evidence in civil and criminal enforcement cases.

The recording will be overt in all circumstances so the subject of the recording will be aware that recording is taking place. The police officer will tell the subject that recording is taking place. There will also be overt signage on the officer to indicate that recording is taking place. The subject will be in a position to choose how they respond to the recording.

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?

South Somerset District Council use the recording submitted by the police in order to enforce the proposed PSPOs.

The intended effect on individuals is to provide the evidence for effective enforcement.

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?

Relevant Stakeholders:

South Somerset Internal Stakeholders

- Locality Team Leader
- Specialist Team Leader
- Specialist within the People team
- Senior Management Team
- Support Service (ICT)
- Strategy & Commissioning: Data Protection

External Stakeholders

- Avon and Somerset Police (Data sharing agreement)

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?

There is a well-established lawful basis for the retention of video evidence for the investigation and enforcement of criminal and civil offences.

The gathering of “real” evidence supports these enforcement functions, streamlines the enforcement process and improves outcomes.

In order to prevent function creep the recordings will only be accessible by authorised personnel and all non-evidential data will be maintained for a maximum of 31 days before it is deleted. Recordings required as evidence will be kept for a maximum of 6 months or until the evidence is no longer required, whichever is longer.

The recording will only be viewed by authorised personnel where evidence exists to support the Councils enforcement functions.

Individuals can request images and information about themselves through a subject access request under the GDPR. Detailed guidance on this and matters such as when to withhold images of third parties caught in images is included in the ICO CCTV code of practice. Detailed guidance on these obligations is included in the ICO CCTV code of practice.

How will you support their rights?

There must be as much transparency in the use and retention of evidence as possible, including a published contact point for access to information, privacy notice and complaints. Individuals will also have the right to complaint to the Information Commissioners Officer if they feel that their rights regarding their personal data have been violated.

How do you ensure processors comply?

Annual review of the system including any notes made when recordings are viewed for the stated purposes.

Step 5: Identify and assess risks

Describe the 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
inability to exercise rights (including but not limited to privacy rights);	Reasonable Possibility	Some impact	Medium
inability to access services or opportunities;	Remote	Some impact	Low
loss of control over the use of personal data;	Reasonable Possibility	Serious harm	High
discrimination;	Reasonable Possibility	Serious harm	High
identity theft or fraud;	Remote	Some impact	Low
financial loss;	Remote	Minimal impact	Low
reputational damage;	Reasonable Possibility	Serious Harm	High
physical harm;	Remote	Some impact	Low
loss of confidentiality;	Reasonable Possibility	Serious Harm	High
re-identification of pseudonymised data;	Remote	Minimal impact	Low
any other significant economic or social disadvantage			

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

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
Inability to exercise rights	<u>Right to privacy</u> • Viewing of recordings restricted to a small pool of people (1). • Viewing of recordings will take place in a private location, such as a meeting room. • Limit retention period to 31 days by default. • Recordings required as evidence will be kept for a maximum of 6 months or until the evidence is no longer required, whichever is longer. <u>Right to access data</u> • Published contact point for access to information on website.	Mitigate risk to a minimum	Low	
Loss of control over the use of personal data	<u>Right to privacy</u> • Viewing of recordings restricted to a small pool of people (1). • Viewing of recordings will take place in a private location such as a meeting room. • Limit retention period to 31 days by default. • Recordings required as evidence will be kept for a maximum of 6 months or until the evidence is no longer required, whichever is longer. <u>Right to access data</u> • Published contact point for access to information on website.	Mitigate risk to a minimum	Low	
Discrimination	<u>Right to privacy</u> • Viewing of recordings restricted to a small pool of people (1). • Viewing of recordings will take place in a private location such as a meeting room.	Mitigate risk to a minimum	Low	

	• Limit retention period to 31 days by default. • Recordings required as evidence will be kept for a maximum of 6 months or until the evidence is no longer required, whichever is longer. <u>Right to access data</u> • Published contact point for access to information on website.			
Reputational damage	<u>Right to privacy</u> • Viewing of recordings restricted to a small pool of people (1). • Viewing of recordings will take place in a private location such as a meeting room. • Limit retention period to 31 days by default. • Recordings required as evidence will be kept for a maximum of 6 months or until the evidence is no longer required, whichever is longer. <u>Right to access data</u> • Published contact point for access to information on website.	Mitigate risk to a minimum	Low	
Loss of confidentiality	<u>Right to privacy</u> • Viewing of recordings restricted to a small pool of people (1). • Viewing of recordings will take place in a private location such as a meeting room. • Limit retention period to 31 days by default. • Recordings required as evidence will be kept for a maximum of 6 months or until the evidence is no longer required, whichever is longer. <u>Right to access data</u> • Published contact point for access to information on website.	Mitigate risk to a minimum	Low	

Surveillance Legislation

European Convention on Human Rights (ECHR)
The ECHR sets out the fundamental rights and freedoms that signatory governments must secure to everyone within their jurisdiction. Article 8 provides a right to respect for an individual's private and family life, home and correspondence.

Intelligence Services Act 1994 (ISA)
The ISA makes provisions for the issue of warrants and authorisations enabling certain actions to be taken by the Intelligence Services in relation to interference with property and wireless telegraphy.

Part III Police Act 1997
Part III Police Act 1997 outlines the requirements for the consideration and authorisation of interference in respect of property and wireless telegraphy.

Human Rights Act 1998 (HRA)
The HRA gives further legal effect in the UK to the fundamental rights and freedoms contained in the ECHR. Its effect is that all public bodies such as police and local governments, and other bodies carrying out public functions, have to comply with an individual's ECHR rights. Among other things it also means that individuals can take human rights cases to domestic courts rather than having to take their case in the European Court of Human Rights.

Regulation of Investigatory Powers Act 2000 (RIPA)
RIPA provides the regulatory framework for determining whether a range of covert investigatory techniques by public authorities is proportionate and necessary in compliance with Article 8 of the ECHR.

Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA)
RIPSA provides the regulatory framework in Scotland for determining whether covert surveillance and the use of covert human intelligence sources by public authorities acting on devolved matters, is proportionate and necessary in compliance with Article 8 of the ECHR.

Protection of Freedoms Act 2012 (PoFA)
The PoFA introduces a code of practice for surveillance camera systems, the appointment of Surveillance Camera and Biometrics Commissioners and provides for judicial approval of certain surveillance activities by local authorities.

Data Protection Act 2018 (DPA)
The DPA regulates the processing of personal data. It provides seven principles of good information handling with which organisations must comply and provides individuals with rights with respect to the processing of their personal data.

General Data Protection Regulation (GDPR)
The GDPR is a Europe-wide law that applies to the use of 'personal information' which means any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier. The GDPR sets out requirements for how organisations need to handle personal data from 25 May 2018.

Step 7: Sign off and record outcomes

Item	Name/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 be kept under review by:		The DPO should also review ongoing compliance with DPIA